Software Version 5.3
August 2014
702P03157

Embedded for Xerox EIP
Setup Guide

Document Version: 1.0 (August 2014)

Table of Contents

1 Introduction

Topics

Xerox Secure Access supports Secure Access Authentication Devices within an Xerox Secure Access environment. In a secure printing Xerox Secure Access environment, users must authenticate at a Secure Access Device before they are allowed to access the supported Xerox MFP controlled by the device.

In addition to authentication, users can select and release secure print documents directly from the MFP front panel.

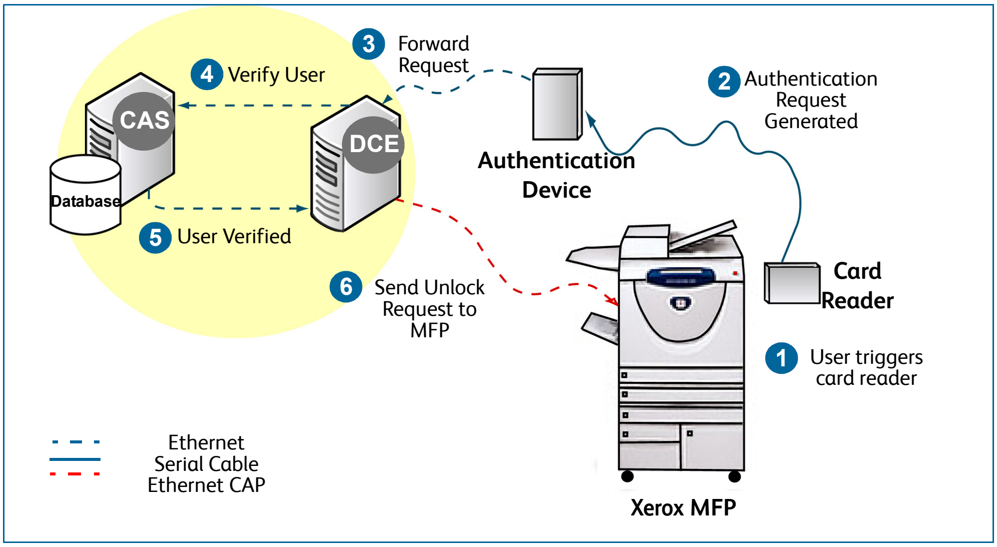
This guide provides instructions to configure the server-side requirements within an Xerox Secure Access environment.

About User Authentication

Xerox Secure Access provides the ability to control access to the print and copy functions of Xerox Multifunction peripheral (MFP) devices. When a user approaches an Xerox-controlled device, they enter user credentials either by using a card, or manually entering data on the MFP front panel. The MFP front panel is unlocked only when the user's account information is authenticated by the accounting server.

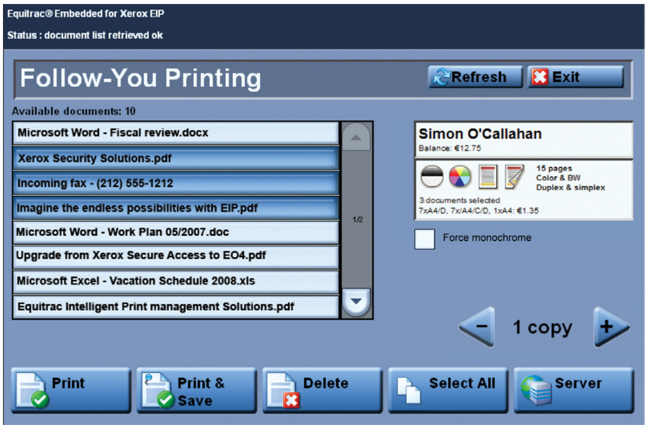
Using a proprietary protocol (Convenience Authentication Protocol), the Authentication Device contacts the accounting server via an Ethernet network connection to verify the user information gathered from the swipe or proximity card. If the accounting server verifies the user, the MFP device panel unlocks and is ready for use. If the user is not verified, the MFP remains locked and the user cannot perform any tasks at the device.

The Device Control Engine (DCE) handles all communication with the MFP devices. When a user wants to use the copy, or fax functionality on a MFP, they must first trigger the card reader. A swipe or proximity read initiates an access request. The Authentication Device forwards the login request to the DCE, which then contacts the Core Accounting Server (CAS) to verify the user account data associated with the card. This process is depicted below.



About Secure Document Release

Secure document release (SDR) holds jobs in the print queue until a user releases them from the MFP panel. When CAS is configured to support SDR, users can view a Follow-You® Printing screen on the MFP via the Release My Documents option. This screen displays queued print jobs for the current user. The user can select one or more jobs and release or delete them directly from the MFP front panel.


Equitrac® Embedded for Xerox EIP

Status : document list retrieved ok

Follow-You Printing

Available documents: 10

- Microsoft Word - Fiscal review.docx
- Xerox Security Solutions.pdf
- Incoming fax - (212) 555-1212
- Imagine the endless possibilities with EIP.pdf
- Microsoft Word - Work Plan 05/2007.doc
- Upgrade from Xerox Secure Access to EO4.pdf
- Microsoft Excel - Vacation Schedule 2008.xls
- Equitrac Intelligent Print management Solutions.pdf

1/2

Simon O'Callahan
Balance: €12.75

15 pages
Color & BW
Duplex & simplex

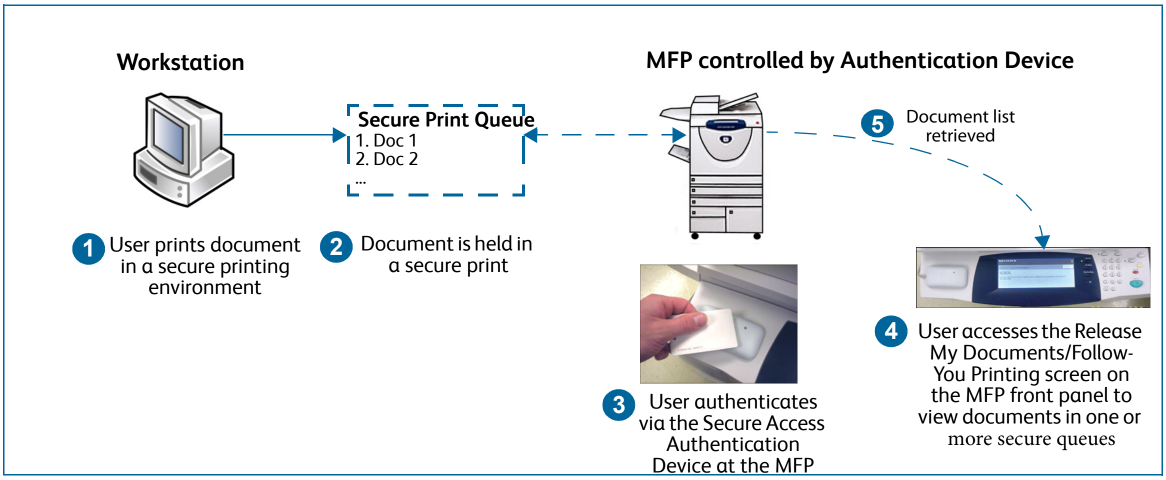
3 documents selected
7xA4/D, 7x/A4/C/D, 1xA4: €1.35

□ Force monochrome

1 copy

If you enable multi-server Follow-You Printing on the CAS, the user can view print jobs on other servers also. For additional information on multi-server Follow-You Printing, refer to the *Advanced Printing Configuration* chapter in the Xerox Secure Access Administration Guide.

The following diagram illustrates the process flow that occurs after a user submits a print job to a controlled queue on a Xerox MFP. After sending the print job, the user goes to a controlled MFP, authenticates via a Secure Access Authentication Device, then uses the Follow-You Printing screen on the front panel to access the Embedded secure document release functions.


Workstation
MFP controlled by Authentication Device
Secure Print Queue
1. Doc 1
2. Doc 2
...
1 User prints document in a secure printing environment
2 Document is held in a secure print
3 User authenticates via the Secure Access Authentication Device at the MFP
4 User accesses the Release My Documents/Follow-You Printing screen on the MFP front panel to view documents in one or more secure queues
5 Document list retrieved

Note

When the Follow-You Printing extension is not configured, the Follow-You Printing screens are not available on the MFP panel and the user cannot select individual jobs for release. After the user authenticates, all jobs are released from the local or home server or workstation.

Installation and Configuration Requirements

If you have already set up and configured your Xerox Secure Access server, you do not need to install the basic Xerox Secure Access application; you only need to follow configuration procedures.

For instructions on installing and configuring Xerox Secure Access, see the *Xerox Secure Access Unified ID System® Installation Guide* and the *Xerox Secure Access Administration Guide.*

Before configuring Xerox Secure Access, you need the following:

- The IP address of the Device Control Engine (DCE) server. You need this address when configuring the MFP to communicate with the DCE server.
- Administrative access to System Manager. For details, see *Configuring Administrative Access* in the Xerox Secure Access Administration Guide.

Licensing, Server, and MFP Requirements

To enable the Embedded solution, you must obtain the following:

- **Xerox Secure Access Software**

Xerox Secure Access requires configuration of the MFPs, the Core Accounting Server (CAS), and the Secure Access Authentication Devices. This guide provides complete setup instructions for all of these components.

- **One Authentication Device per controlled Xerox MFP**

Each MFP is controlled by an Authentication Device, comprised of an authentication terminal and card reader. See Authentication Device Component Requirements on page 5 for details.

- **One embedded license per Xerox MFP**

Each Secure Access Authentication Device requires an embedded license applied in System Manager. For example, if you plan to control 20 Xerox MFPs, you need to obtain 20 corresponding embedded licenses (enabled for Xerox). See Licensing Embedded Devices on page 2 for instructions on adding licenses to the CAS.

- **EIP-enabled Xerox MFPs**

If you are not certain whether your MFPs meet this requirement, contact Xerox for further details. Visit http://www.nuance.com/for-business/by-product/equitrac/supported-devices/xerox/index.htm for a list of supported MFP models.

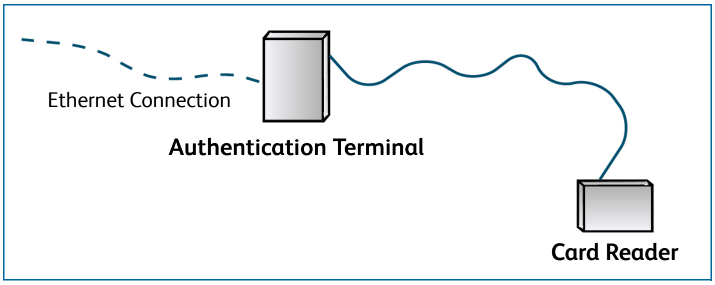
- **One Network Accounting Enablement Option per Xerox MFP**

Only required if you are tracking copy, or fax usage. This is NOT required to track printing if you are using Equitrac® printer ports.

This licensable device option obtained from Xerox enables the Xerox MFP to automatically track print, server fax and copy usage for each account.

Authentication Device Component Requirements

A Secure Access Authentication Device is comprised of an Authentication Terminal and an external card reader. When connected to an external card reader, the Authentication Terminal controls user access to the MFP. The user must swipe or pass a card through or near the card reader, and validate user credentials against the accounting server before the MFP is available for use.



Ensure that you have all the hardware provided with each Authentication Device:

- Power supply
- Power cable
- Bypass (Reset) key (metal key used to reset the device to defaults) See Resetting an Authentication Device on page 7.
- 10/100 Base-T Ethernet network cable
- Card Reader

System Requirements

To review the system requirements for the machine or machines hosting the Core Accounting Server and Device Control Engine server components, see the *Xerox Secure Access Unified ID System® Installation Guide*.

Supported MFPs

For a list of Xerox Secure Access supported MFP models, visit http://www.nuance.com/for-business/by-product/equitrac/supported-devices/xerox/index.htm.

Note

Newer models of Xerox MFP may be able to use Xerox ECSP. Xerox ECSP is able to leverage the displays and processing power of late-model Xerox MFPs to offer enhanced features. Xerox ECSP is a different platform than Xerox EIP, and has different requirements. **If your device(s) use Xerox ECSP, please consult the *Embedded for Xerox ESCP* documentation instead of this guide.**

Supported MFP models must be EIP-enabled prior to installing the Xerox Secure Access solution. Please contact your local Xerox Sales Representative for more information.

Supported Card Readers

For a list of Xerox Secure Access supported card readers, visit http://www.equitrac.com/card_readers.html.

All card readers are pre-configured from the manufacturer and require no further configuration.

Magstripe Device Reader

Xerox Secure Access supports external magnetic stripe reader devices. Users can enter validation data by swiping an encoded magnetic card through the card reader. The reader reads virtually any standard magnetic card medium on track 2, and accepts standard or custom encoded data.

Proximity and Contactless Smart Cards

Xerox Secure Access supports HID proximity cards, and Mifare and Legic contactless smart cards. Users can enter validation data by passing the card within about one inch of the card reader.

Additional Documentation

You may need to refer to one of the following documents when performing server-side configuration tasks. These documents are located on the Xerox Secure Access product CD, and are installed automatically with any server-side component in the Program Files\Equitrac\MPS\Docs folder.

Guide	When to refer to this guide
Xerox Secure Access Installation Guide	Use this guide to perform an initial installation or upgrade.
Xerox Secure Access Administration Guide	After installing Xerox Secure Access, use this guide to configure advanced options for use on your campus or in your organization.

List of Terms

The following unique terms are used within this guide.

Term	Description
Alternate Primary PIN	A sequence of personal identification numbers that uniquely identifies a user who wants to release a print job. The alternate primary PIN can be data encoded on a magnetic swipe card or entered into an MFP keypad.
Authentication	The process of entering a primary and optional secondary personal identification number to gain access to a controlled MFP. Users can authenticate via a card reader, or through the MFP control panel.

Term	Description
Core Accounting Server (CAS)	The Core Accounting Server is a core component of Xerox Secure Access. This service controls the accounting database that stores all printer, user, transaction and balance information. The CAS also verifies users, calculates printing charges and assigns charges to an appropriate user.
Convenience Authentication	A protocol that enables communication between the Authentication Device and the Xerox server to verify user information gathered from a swipe or proximity card.
Device Control Engine (DCE)	A core component of Xerox Secure Access, the DCE communicates with terminals that control access to MFPs.
Device Routing Engine (DRE)	A core component of Xerox Secure Access, the DRE enables document flow from workstations to output devices. When a job is released, the DRE captures the job characteristics and communicates the characteristics to the CAS.
Follow-You Printing	A secure printing feature that holds print jobs in a virtual print queue until the user "pulls" the print job to a selected device. A user can select a particular printer when they submit a print request, then walk to an entirely different compatible MFP and pull the job to that device.
Follow-You Printing screen	An additional screens that appears as a custom service on the MFP when the Follow-You Printing extension is configured. Users can select one or more jobs from different print servers.
Multi-server Follow-You	A secure printing feature that extends the Follow-You functionality to allow users to view and release secure print jobs from different print servers.
Network Accounting	A feature of the Xerox MFP which automatically tracks print, server, fax and copy usage for each user. Network accounting is run over a network and the accounting transactions are performed remotely by Xerox Secure Access server software.
Print Tracking	The ability to track the attributes of a released network print job. For example, number of pages, page size, color, etc. You can configure Xerox Secure Access to track printing through the embedded device or through an Equitrac Port.
Primary PIN	A sequence of numbers that act as a user ID to uniquely identify a user who wants to release a print job. The primary PIN can be entered on the MFP keypad.
Secondary PIN	A sequence of numbers that act as a password when used in conjunction with a Primary PIN. After entering the Primary PIN, the user must enter the Secondary PIN code on a MFP keypad before the print job is released to a device. Secondary PINs are an optional configuration.
Secure Document Release (SDR)	An Xerox Secure Access feature that holds network print jobs in a secure virtual print queue. Users must authenticate at an MFP to release jobs from the secure queue. The goal of secure printing is to ensure that proprietary information does not sit at an output device for public consumption.

MFP Configuration

2

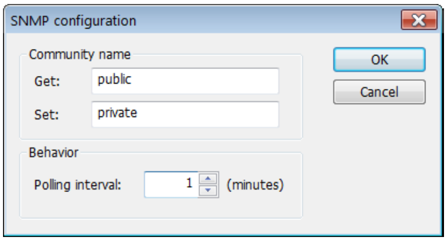
Topics

To enable Xerox Secure Access, you must configure the MFPs. Follow the steps for each MFP series in the order they are presented to ensure a successful install.

Configuring MFP Properties

The following are the main steps when configuring Xerox MFPs:

1. Ensure that the time zone on the MFP is correct. if the time zone is not correct, Xerox Embedded transaction times are incorrectly reported.
2. Confirm that the date and time setting on the MFP is within 24 hours of the date and time configured on the server that hosts the DCE component. If the settings are more than 24 hours apart, the Embedded application on the MFP will not connect to the server.
3. Configure the MFP to use Secure Access Authentication and to communicate with the DCE Server.
4. Ensure that the SNMPv2 settings on the device are correct. Read-only (Get) and Read and Write (Set) community names must be configured as **public** and **private** respectively. Note that all characters must be entered in lower case. Also ensure that these SNMP settings are enabled in **System Manager > Configuration > SNMP configuration**.



SNMP configuration

Community name

Get: public

Set: private

Behavior

Polling interval: 1 (minutes)

5. Ensure **SSL** is enabled on the Xerox MFP. If it is not enabled, generate a self-signed certificate and then enable SSL communication.
6. Verify the firmware version on the Xerox MFP. MFPs running EIP firmware versions 1.5 and 2.0 require that the Embedded Manual Override is Enabled in order for the attached card reader to operate normally. Contact your local Xerox representative for information on the appropriate firmware for your MFPs. Refer to WorkCentre 75xx Series on page 11 for details on enabling this option.

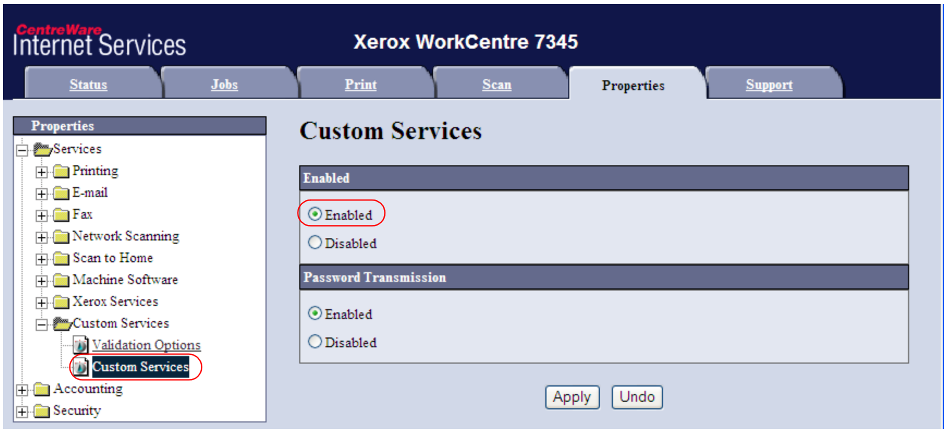
WorkCentre 52xx, 7232/7242, 73xx, and 74xx Series

All configuration of the WorkCentre 52xx, 7232/7242, and 73xx MFPs is performed via the Internet Services interface. No configuration at the MFP console is required.

Note

If prompted to reboot during this process, reboot and resume configuration at the next step.

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **Services** folder, then the **Custom Services** subfolder, and then **Custom Services**.



Custom Services

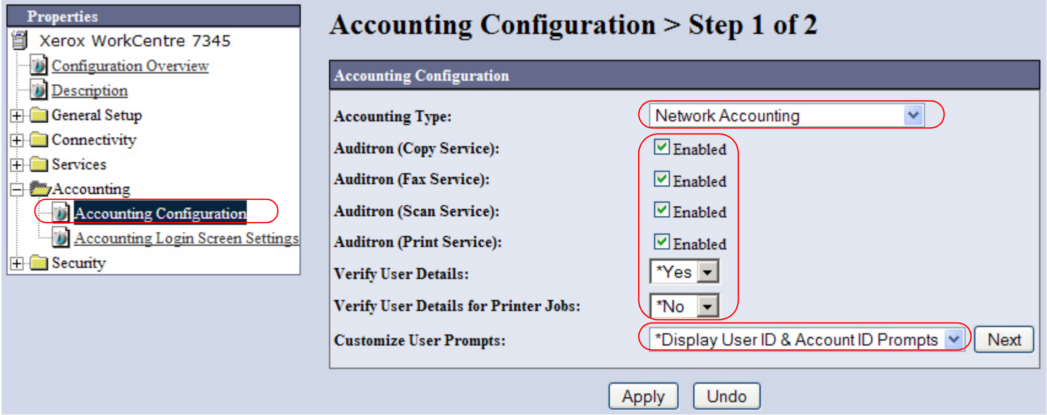
Enabled

● Enabled
○ Disabled

Password Transmission

● Enabled
○ Disabled

4. In the right pane, ensure that **Custom Services** is set to **Enabled**, then click **Apply**. The Custom Services button should now be present on the MFP user interface when All Services is selected.
5. In the left pane, select the **Accounting** folder, then the **Accounting Configuration** subfolder.



Accounting Configuration > Step 1 of 2

Accounting Configuration

Accounting Type:	Network Accounting
Auditron (Copy Service):	☑ Enabled
Auditron (Fax Service):	☑ Enabled
Auditron (Scan Service):	☑ Enabled
Auditron (Print Service):	☑ Enabled
Verify User Details:	*Yes
Verify User Details for Printer Jobs:	*No
Customize User Prompts:	*Display User ID & Account ID Prompts

6. In the **Authentication Configuration > Step 1 of 2** page, set the following options:
   a. Select **Network Accounting** from the **Accounting Type** drop-down list.
   b. Enable the services you want to track on this MFP: **Copy, Fax, and Print**.
   c. Select **Yes** from the **Verify User Details** drop-down list.
   d. Select No from the **Verify User Details for Printer Jobs** drop-down list. (Jobs will not print if set to Yes.)

Note

For models 72x2 with older firmware, it may be necessary to set the *Verify User Details* option to *No* in order to avoid transactions being recorded against “Unidentified user”.

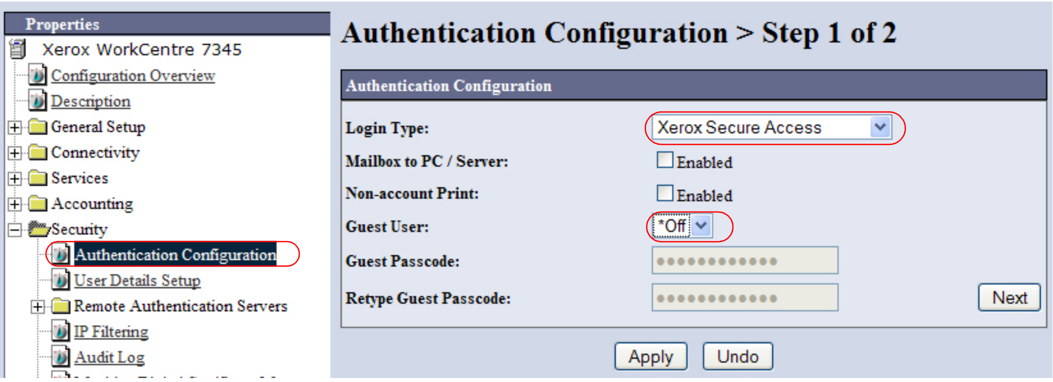
e. Select **Display User ID & Account ID Prompts** from the **Customize User Prompts** drop-down list. Failure to set this option causes transactions to be recorded against “Unidentified user”.

7. Click **Apply** to save these settings.
8. Click **Reboot Machine**, if prompted.

Caution

While the MFP is rebooting, do NOT click anywhere on the web page, as an error message indicating that services are unavailable will appear. If this occurs, once the device is back online, you will need to login again to the web page and navigate to the applicable menu before continuing.

9. In the left pane, select the **Security** folder, then the **Authentication Configuration** subfolder.



Authentication Configuration > Step 1 of 2

Authentication Configuration

Login Type: Xerox Secure Access

Mailbox to PC / Server: □ Enabled

Non-account Print: □ Enabled

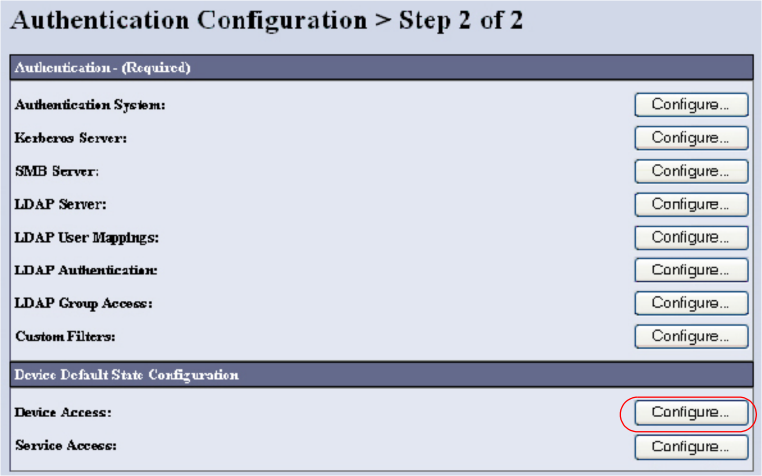
Guest User: *Off

Guest Passcode: ••••••••••••

Retype Guest Passcode: ••••••••••••

10. In the **Authentication Configuration > Step 1 of 2** page, set the following options:
    a. Select **Xerox Secure Access from** the **Login Type** drop-down list.
    b. Select **Off** from the **Guest User** drop-down list.
    c. Leave all other options unchanged.

11. Click **Apply** to save the settings.
12. Reboot the machine when prompted. Do NOT click anywhere on the web page until the reboot is complete.
13. Click **Next** to continue to the **Authentication Configuration >** Step 2 of 2 page.
14. To lock the front panel of the MFP, click the **Configure** button beside the **Device Access** option.



Authentication Configuration > Step 2 of 2

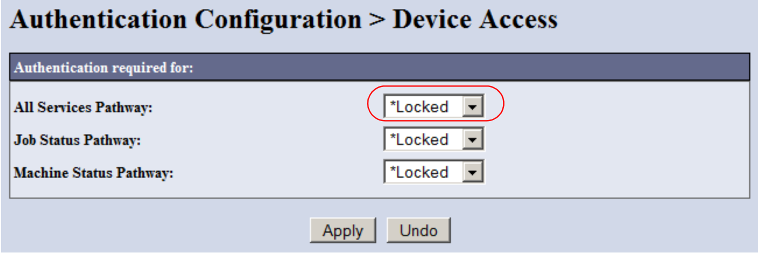
Authentication - (Required)

Authentication System: Configure...
Kerberos Server: Configure...
SMB Server: Configure...
LDAP Server: Configure...
LDAP User Mappings: Configure...
LDAP Authentication: Configure...
LDAP Group Access: Configure...
Custom Filters: Configure...

Device Default State Configuration

Device Access: Configure...
Service Access: Configure...

15. Set the **All Services Pathway** to **Locked**, and then click **Apply**.

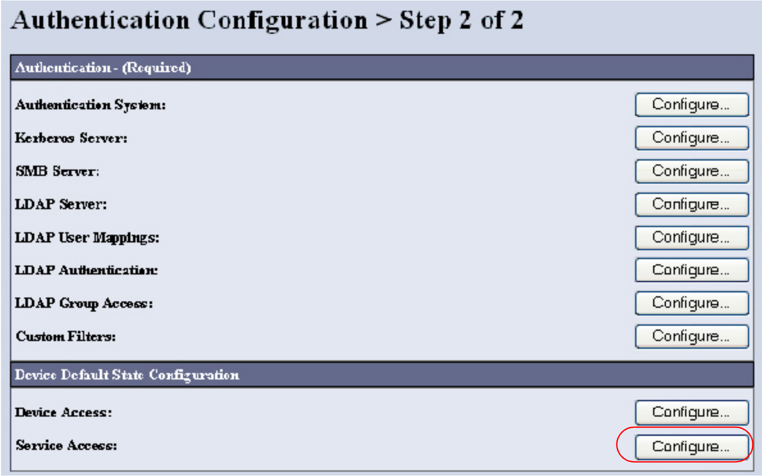


Authentication Configuration > Device Access

Authentication required for:

All Services Pathway: *Locked
Job Status Pathway: *Locked
Machine Status Pathway: *Locked

16. Reboot the machine when prompted. Do NOT click anywhere on the Web page until the reboot is complete.
17. To lock some, but not all, of the Services, click the **Configure** button located beside the **Service Access** option.



Authentication Configuration > Step 2 of 2

Authentication - (Required)

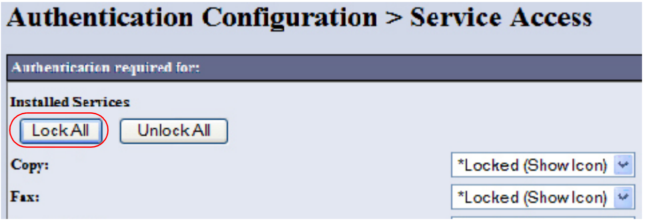
Authentication System: Configure...
Kerberos Server: Configure...
SMB Server: Configure...
LDAP Server: Configure...
LDAP User Mappings: Configure...
LDAP Authentication: Configure...
LDAP Group Access: Configure...
Custom Filters: Configure...

Device Default State Configuration

Device Access: Configure...
Service Access: Configure...

18. On the Service Access page, select the services you want to control access to, then click **Save**.

- **Locked (Show Icon)** - the service appears on the MPF control panel, but cannot be accessed without authentication.
- **Unlocked** - the service appears on the control panel and is accessible without authentication.



Authentication Configuration > Service Access

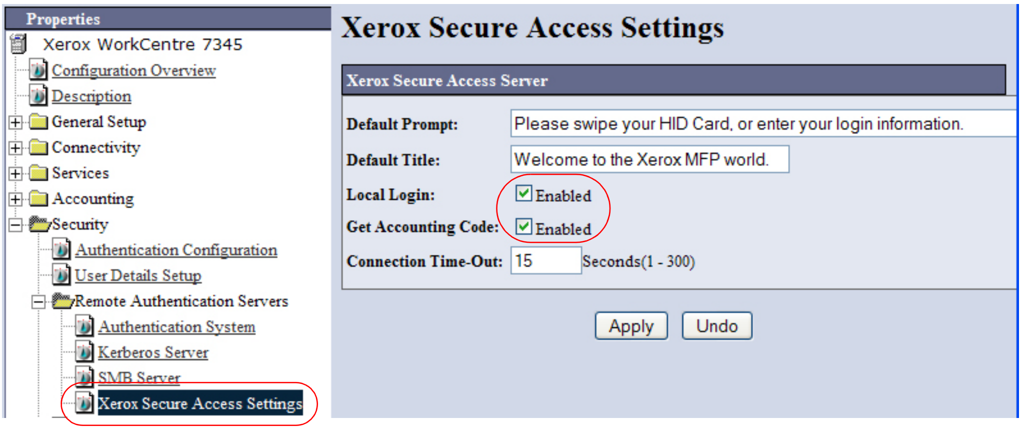
Authentication required for:

Installed Services

Copy: *Locked (Show Icon)

Fax: *Locked (Show Icon)

19. Click the **Apply** button to save all of the Configuration Authentication settings.
20. In the left pane, select the **Security** folder, then the **Remote Authentication Servers** subfolder, and then **XeroxSecureAccess Settings**.



Xerox Secure Access Settings

Xerox Secure Access Server

Default Prompt: Please swipe your HID Card, or enter your login information.

Default Title: Welcome to the Xerox MFP world.

Local Login: ☑ Enabled

Get Accounting Code: ☑ Enabled

Connection Time-Out: 15 Seconds(1 - 300)

21. In the Xerox Secure Access Settings page in the right pane, set the following options:

    a. Set **Local Login** to **Enabled** (checked) if you want to make the keyboard access button visible.

    Note

    Although the Local Login setting is optional, ensure that you check this option at first configuration. After first initialization, this option can only be enabled if the device is cleared from all settings (back to the factory defaults).

    b. Set **Get Accounting Code** to **Enabled** (checked). You must select this option to enable authentication.

    c. Set the **Connection Time-Out** value to at least **15** seconds, or a larger value to avoid timeout messages on the MFP.
22. Click **Apply** to save these settings and to complete the configuration of this MFP
23. Click **Reboot Machine**, then close the web browser.

WorkCentre 56xx Series

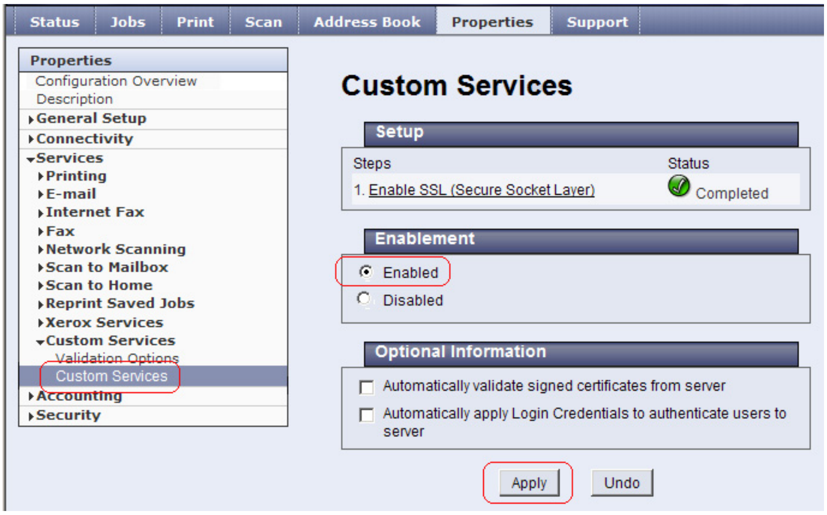
You must configure the WorkCentre 56xx series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **General Setup** folder, then select the **Custom Services Setup** subfolder.
   - If it says **Configured** beside **Custom Service Registration** the option is enabled.
   - If it says **Not Configured**, click the **Configure** button and click the **Custom Services Registration** option. Click the **Save** button.
4. In the **Enable Custom Services** section, select the **Display Custom Services Section** button at the local user interface option.
5. In the Browser Settings section, select the Enable the Custom Services Browser option. If you do not enable this option, nothing will happen when you press the button.

   Caution

   If the services are not installed, contact Xerox regarding custom services installation.
6. In the right pane, ensure that **Custom Services** is set to **Enabled**, then click **Apply**. The Custom Services button should now be present on the MFP user interface when All Services is selected.



Custom Services

Setup

Steps	Status
1. Enable SSL (Secure Socket Layer)	✓ Completed

Enablement

● Enabled

○ Disabled

Optional Information

□ Automatically validate signed certificates from server

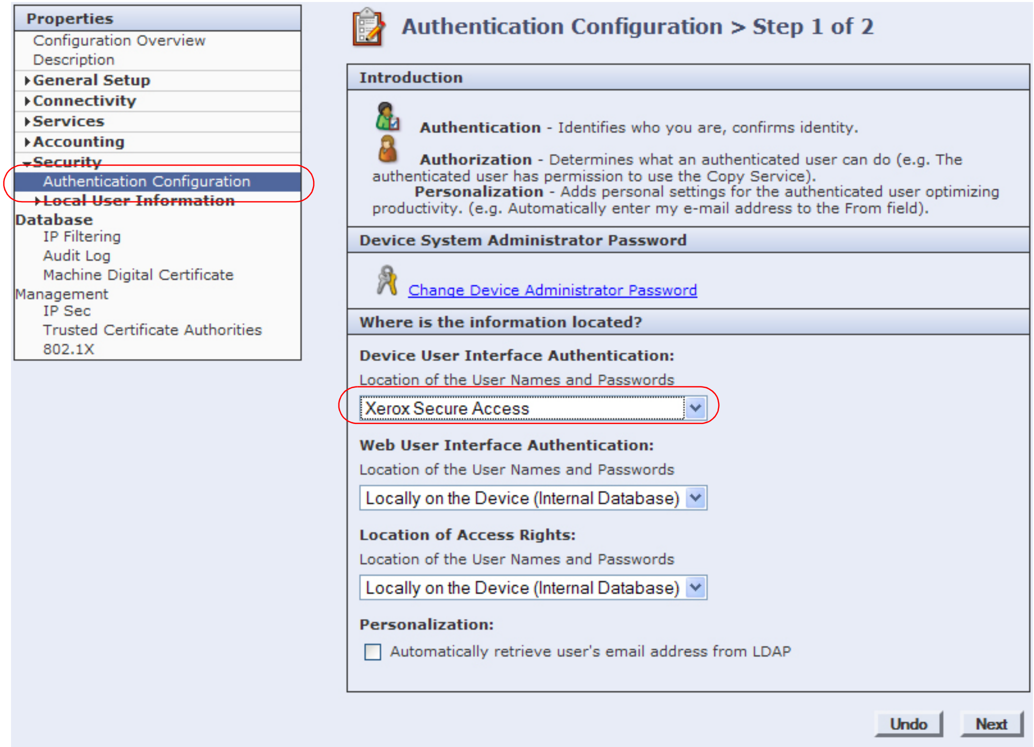
□ Automatically apply Login Credentials to authenticate users to server

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Touch **Access and Accounting**.
4. Touch **Authentication Mode**.
5. Under Network Accounting, touch the **On** option to enable Network Accounting. Ensure that all other authentication options are disabled. Touch **Save**.
6. Return to the **Access and Accounting** menu, then touch **Network Accounting Setup**.
7. Touch **Network Accounting Authentication**.
8. Exit the Tools screen, and return to copy mode. Configuration on the MFP console is now complete.

Via the Internet Services Interface

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **Security** folder, then select **Authentication Configuration**.



Authentication Configuration > Step 1 of 2

Introduction

Authentication - Identifies who you are, confirms identity.

Authorization - Determines what an authenticated user can do (e.g. The authenticated user has permission to use the Copy Service).

Personalization - Adds personal settings for the authenticated user optimizing productivity. (e.g. Automatically enter my e-mail address to the From field).

Device System Administrator Password

Change Device Administrator Password

Where is the information located?

Device User Interface Authentication:
Location of the User Names and Passwords
Xerox Secure Access

Web User Interface Authentication:
Location of the User Names and Passwords
Locally on the Device (Internal Database)

Location of Access Rights:
Location of the User Names and Passwords
Locally on the Device (Internal Database)

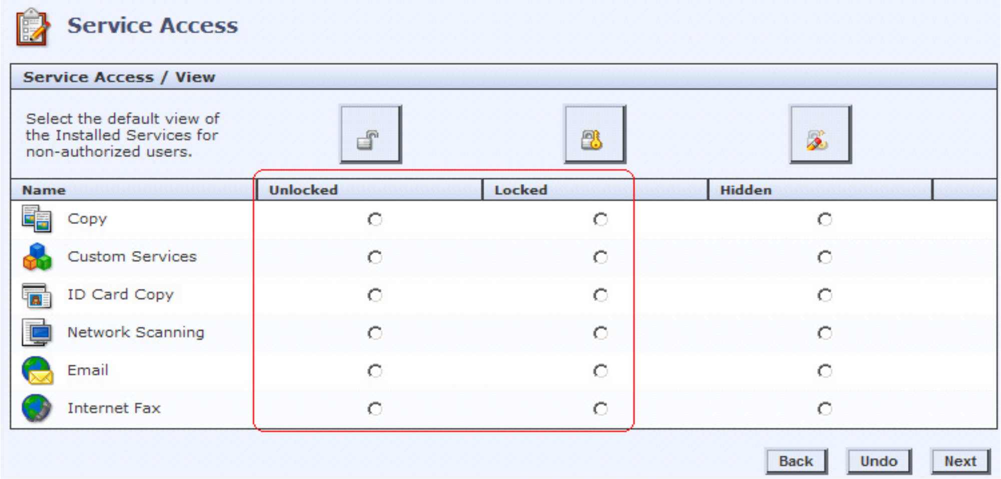
Personalization:
□ Automatically retrieve user's email address from LDAP

4. In the **Where is the information located** section, select **Xerox Secure Access from** the **Device User Interface Authentication** drop-down list, and the click **Next**.

Note

If the MFP device is in Sleep mode, click the **Exit Sleep Mode** button to wake the device.

5. Click the **Edit** button beside the **Access Setup Wizard** option.
6. In the **Pathway Services** section, select the services you want to control access to, then click **Save**.
7. In the **Installed Services Pathway Access** section, select Locked under Services Pathway and click the Finished button to lock everything on the device. To lock only certain features, leave **Services Pathway** set to **Unlocked** and click the **Next** button. Select the services you want to control access to, then click Save.
    - Unlocked - the service appears on the control panel and is accessible without authentication.
    - **Locked** - the service appears on the MPF control panel, but cannot be accessed without authentication.
    - **Hidden** - the service does not appear on the control panel.



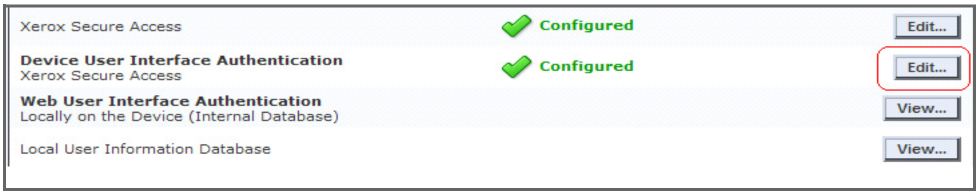
Service Access

Service Access / View

Select the default view of the Installed Services for non-authorized users.

Name	Unlocked	Locked	Hidden
Copy	○	○	○
Custom Services	○	○	○
ID Card Copy	○	○	○
Network Scanning	○	○	○
Email	○	○	○
Internet Fax	○	○	○

8. Still on the Authentication Configuration page, click the **Edit** button beside the **Device User Interface Authentication** option.



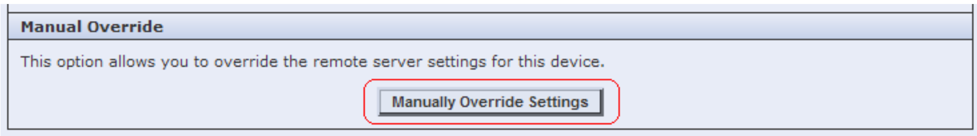
Xerox Secure Access ✓ Configured Edit...

Device User Interface Authentication
Xerox Secure Access ✓ Configured Edit...

Web User Interface Authentication
Locally on the Device (Internal Database) View...

Local User Information Database View...

9. Click the **Manual Override Settings** button at the bottom of the page



Manual Override

This option allows you to override the remote server settings for this device.

Manually Override Settings

10. Under **Device Log In Methods**, select the preferred method:
    - Xerox Secure Access Device Only – if you do not want people to use the alternate key board login button to enter their user ID
    - Xerox Secure Access Device + alternate on-screen authentication method – if you want people to also be able to use the alternate key board login button to enter their user ID
11. Under **Accounting Information (Requires Network Accounting),** select Automatically apply Accounting Codes from the server. This prevents additional unnecessary authentication prompts.
12. Click the **Save** button.
13. Logout of the MFP's configuration utility and close the web browser.

WorkCentre 75xx Series

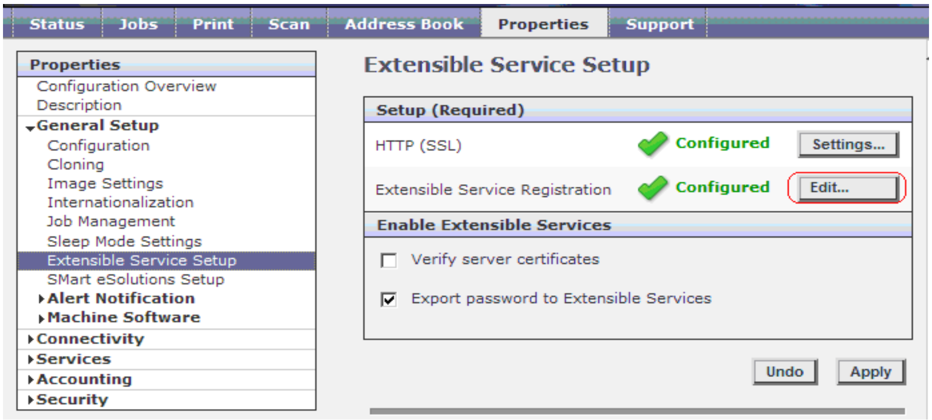
The WorkCentre 75xx series MFPs utilize the Job Limits functionality to support Copy Stop enforcement. The MFP scans the copy job, collects the job information in a JBA (Job-based Accounting) style record and sends it to the server for approval. The server approves or rejects the job depending upon the funds available, color quotas, and copy/print rules. The user balance is updated as each job is copied. The Copy Stop is enforced at the start or during the session.

You must configure the WorkCentre 75xx series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

Xerox EIP cannot be configured unless Custom Service is installed on the MFP. To determine if custom services is installed on a WorkCentre 75xx series, perform these steps:

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **General Setup** folder, then select **Extensible Service Setup**.
4. Click the **Edit** button beside the **Extensible Service Registration** option.



Extensible Service Setup

Setup (Required)

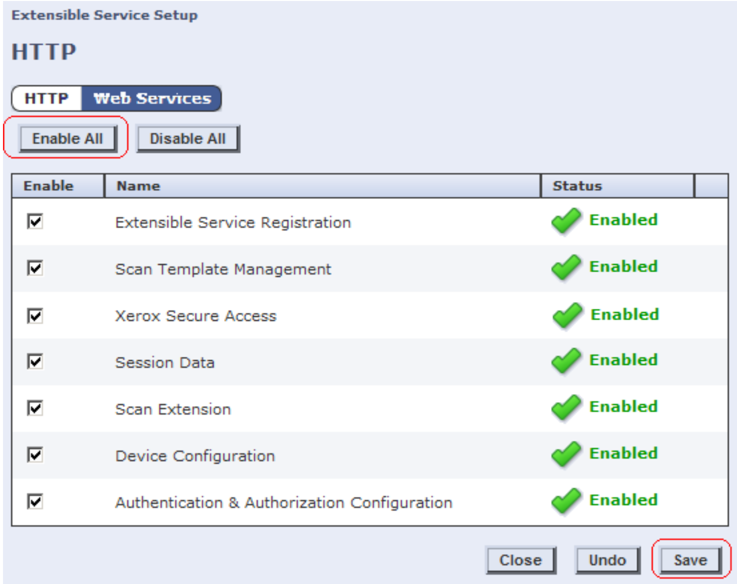
HTTP (SSL)	✓ Configured	Settings...
Extensible Service Registration	✓ Configured	Edit...

Enable Extensible Services

☐ Verify server certificates

☑ Export password to Extensible Services

5. Click on **Enable All**, then click **Save**. The Custom Services button should now be present on the MFP user interface when All Services is selected.



Extensible Service Setup

HTTP

Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	Scan Template Management	✓ Enabled
☑	Xerox Secure Access	✓ Enabled
☑	Session Data	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	Device Configuration	✓ Enabled
☑	Authentication & Authorization Configuration	✓ Enabled

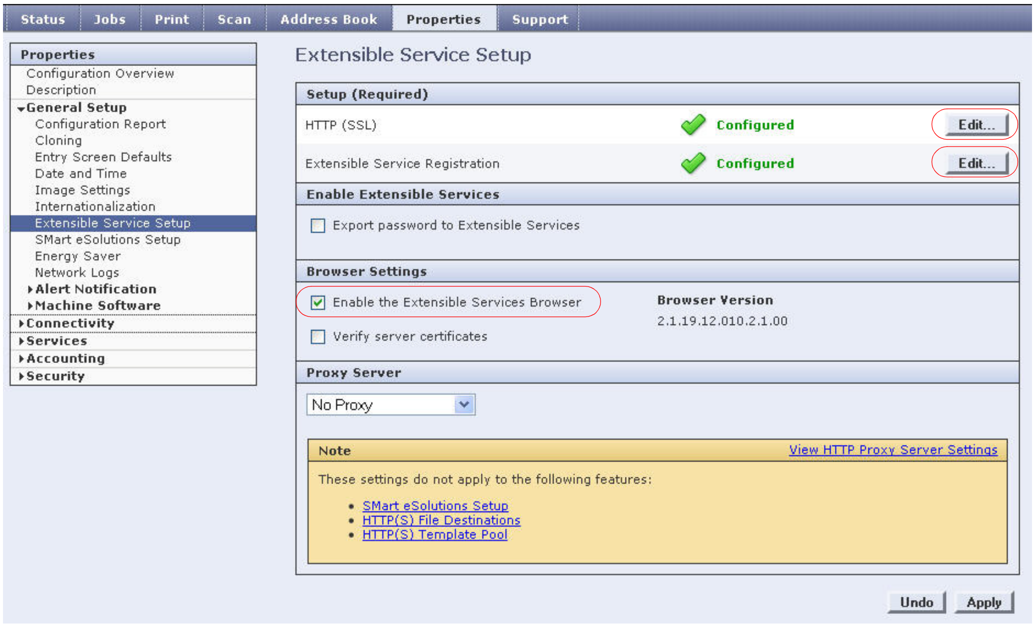
If you cannot access or locate these options, contact Xerox regarding correct installation of Custom Services.

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Enter the user name and password.
4. On the Machine Status screen, touch the **Tools** tab.
5. Touch **Accounting Settings > Accounting Mode**.
6. On the Accounting Mode screen, touch **Network Accounting**, then touch **Customize Prompts**.
7. On the Customize User Prompts screen, touch **Display Prompt 1 and 2,** then touch **Save**. Failure to set this option causes transactions to be recorded against “Unidentified user”.
8. Set **Code Entry Validation** to **Disabled**.
9. Touch the **Save** button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.

Via the Internet Services Interface

1. Open a Web browser and enter the URL `http://`**<MFP IP address>** in the Address field.
2. Select the **Properties** tab, and login with you User ID and Password when prompted.
3. In the left pane, click the **General Setup** folder, then select **Extensible Service Setup**.



Extensible Service Setup

Setup (Required)

HTTP (SSL)	✓ Configured	Edit...
Extensible Service Registration	✓ Configured	Edit...

Enable Extensible Services

□ Export password to Extensible Services

Browser Settings

☑ Enable the Extensible Services Browser

□ Verify server certificates

Browser Version
2.1.19.12.010.2.1.00

Proxy Server

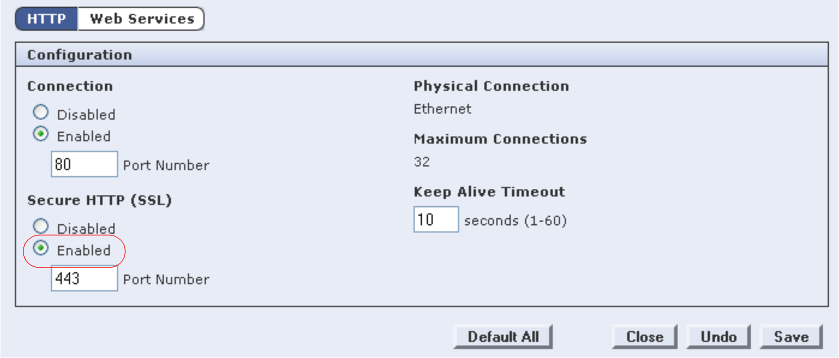
No Proxy

Note

These settings do not apply to the following features:

- SMart eSolutions Setup
- HTTP(S) File Destinations
- HTTP(S) Template Pool

4. Click the **Edit** button beside the **HTTP (SSL)** option.
5. Set the **Secure HTTP (SSL)** option to **Enabled,** then click **Save**.



Configuration

Connection
○ Disabled
● Enabled
80 Port Number

Secure HTTP (SSL)
○ Disabled
● Enabled
443 Port Number

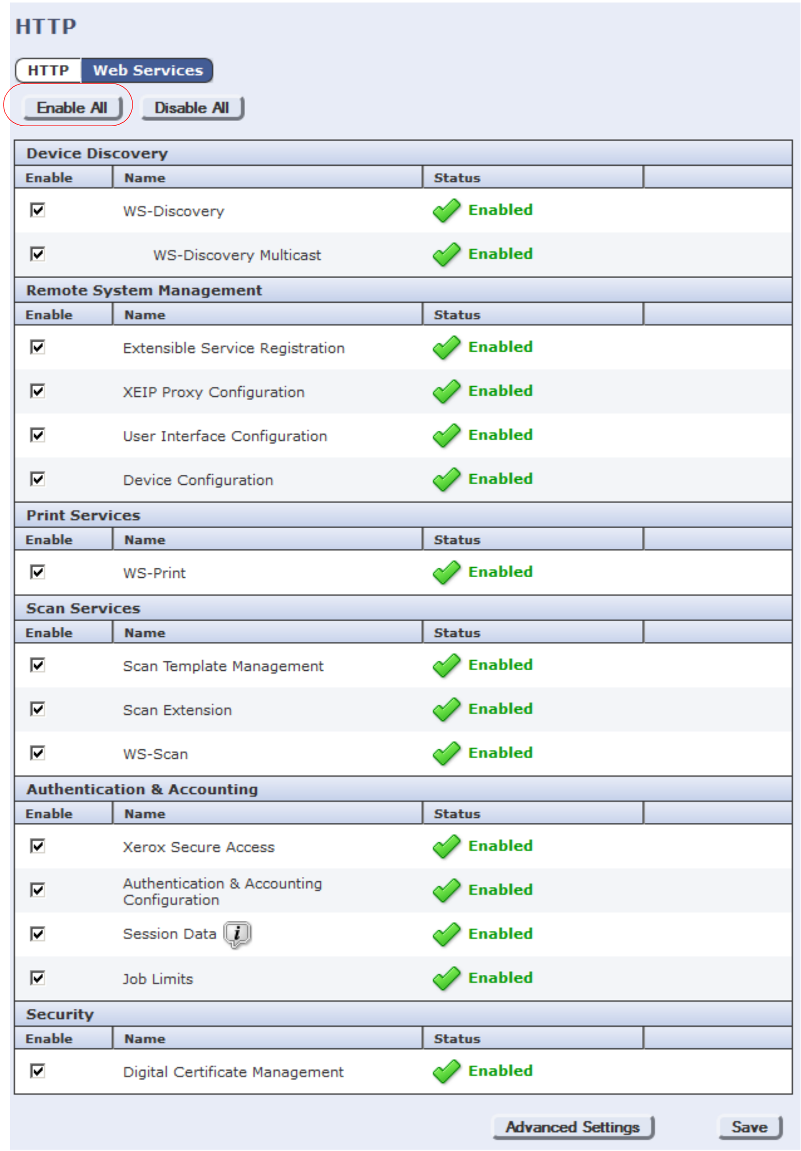
Physical Connection
Ethernet

Maximum Connections
32

Keep Alive Timeout
10 seconds (1-60)

6. Click the **Edit** button beside the **Extensible Service Registration** option.

7. Click **Enable All,** then click **Save**.



Enable	Name	Status
Device Discovery		
☑	WS-Discovery	✓ Enabled
☑	WS-Discovery Multicast	✓ Enabled
Remote System Management		
☑	Extensible Service Registration	✓ Enabled
☑	XEIP Proxy Configuration	✓ Enabled
☑	User Interface Configuration	✓ Enabled
☑	Device Configuration	✓ Enabled
Print Services		
☑	WS-Print	✓ Enabled
Scan Services		
☑	Scan Template Management	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	WS-Scan	✓ Enabled
Authentication & Accounting		
☑	Xerox Secure Access	✓ Enabled
☑	Authentication & Accounting Configuration	✓ Enabled
☑	Session Data	✓ Enabled
☑	Job Limits	✓ Enabled
Security		
☑	Digital Certificate Management	✓ Enabled

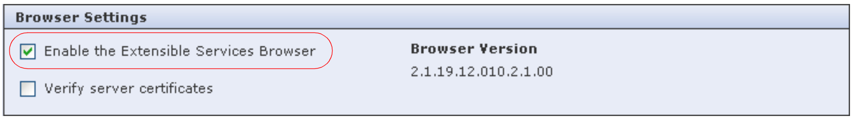
Ensure that both **Authentication & Accounting Configuration** and **Job Limits** are enabled. They are enabled by default. These services must be enabled via the Internet Services interface—not through the physical device.

If these services are not enabled, errors occur when initializing the Xerox embedded device in System Manager, causing the Copy Stop feature to not work.

Note

Job Limits is not supported on all Xerox devices.

8. In the **Browser Settings** section on the Extensible Service Setup page, select the **Enable the Extensible Services Browser** checkbox. and click **Apply**.



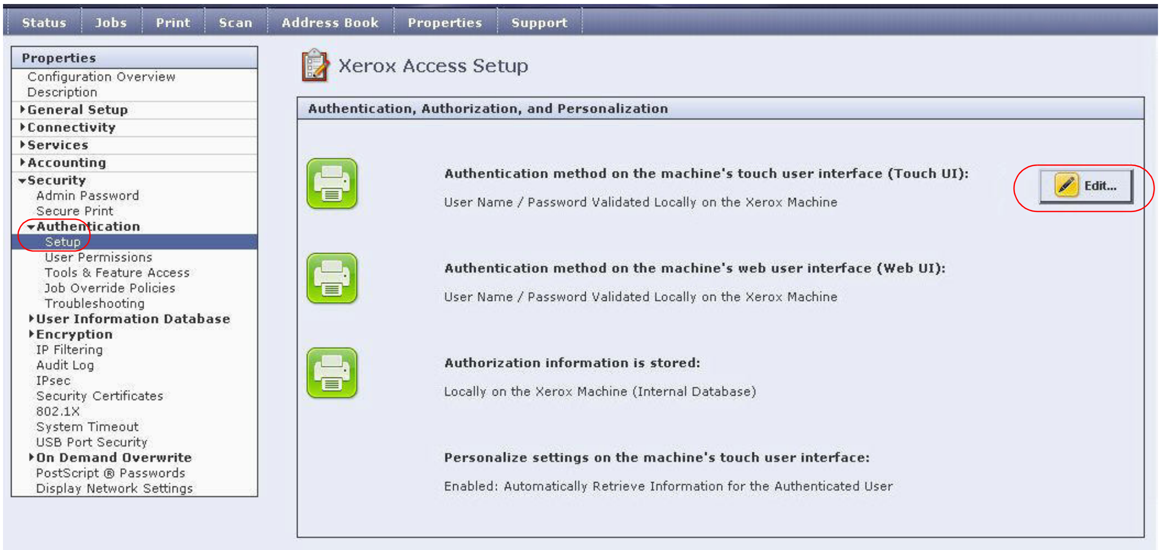
Browser Settings

☑ Enable the Extensible Services Browser

□ Verify server certificates

Browser Version
2.1.19.12.010.2.1.00

9. In the left pane, click the **Security** folder, then the **Authentication** subfolder, and then **Setup.**
10. On the Xerox Access Setup page, click the **Edit** button to change the Authentication method.



Xerox Access Setup

Authentication, Authorization, and Personalization

Authentication method on the machine's touch user interface (Touch UI):
User Name / Password Validated Locally on the Xerox Machine

Authentication method on the machine's web user interface (Web UI):
User Name / Password Validated Locally on the Xerox Machine

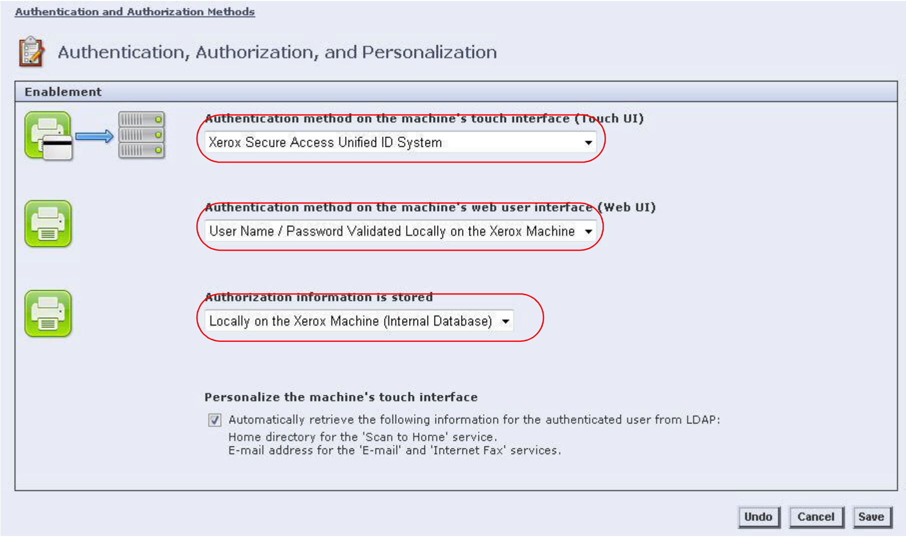
Authorization information is stored:
Locally on the Xerox Machine (Internal Database)

Personalize settings on the machine's touch user interface:
Enabled: Automatically Retrieve Information for the Authenticated User

Note

If the copier has not been previously configured, you may need to click the **Next** button (instead of **Edit)** and then work through a wizard to configure the copier.

11. On the Authentication, Authorization and Personalization page, do the following:



Authentication, Authorization, and Personalization

Enablement

Authentication method on the machine's touch interface (Touch UI)
Xerox Secure Access Unified ID System

Authentication method on the machine's web user interface (Web UI)
User Name / Password Validated Locally on the Xerox Machine

Authorization information is stored
Locally on the Xerox Machine (Internal Database)

Personalize the machine's touch interface
☑ Automatically retrieve the following information for the authenticated user from LDAP:
Home directory for the 'Scan to Home' service.
E-mail address for the 'E-mail' and 'Internet Fax' services.

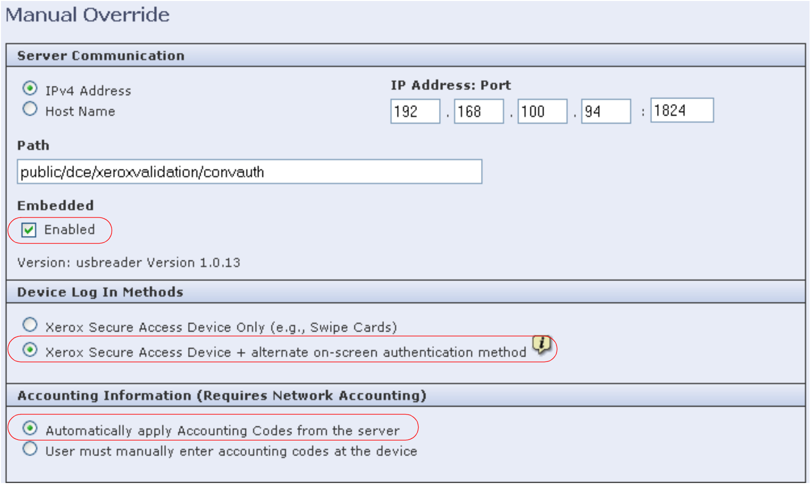
a. Select **Xerox Secure Access Unified ID System** from the **Authentication method on the machine's touch interface** drop-down list.

b. Select **User Name/Password Validated Locally on the Xerox Machine** from the **Authentication method on the machine's web user interface** drop-down list.

c. Select **Locally on the Xerox Machine** from the **Authorization information is stored** drop-down list.

d. Click **Save** to apply the changes.

12. On the Xerox Access Setup page, click the **Edit** button beside the **Xerox Secure Access Setup** option under Configuration Setting.
13. On the Xerox Secure Access Setup page, click the **Manually Override Settings** button.
14. On the Manual Override page, set the following:



Manual Override

Server Communication

● IPv4 Address
○ Host Name

IP Address: Port

192 . 168 . 100 . 94 : 1824

Path

public/dce/xeroxvalidation/convauth

Embedded

☑ Enabled

Version: usbreader Version 1.0.13

Device Log In Methods

○ Xerox Secure Access Device Only (e.g., Swipe Cards)
● Xerox Secure Access Device + alternate on-screen authentication method

Accounting Information (Requires Network Accounting)

● Automatically apply Accounting Codes from the server
○ User must manually enter accounting codes at the device

a. In the **Server Communication** section, set the **Embedded** option to **Enabled**.

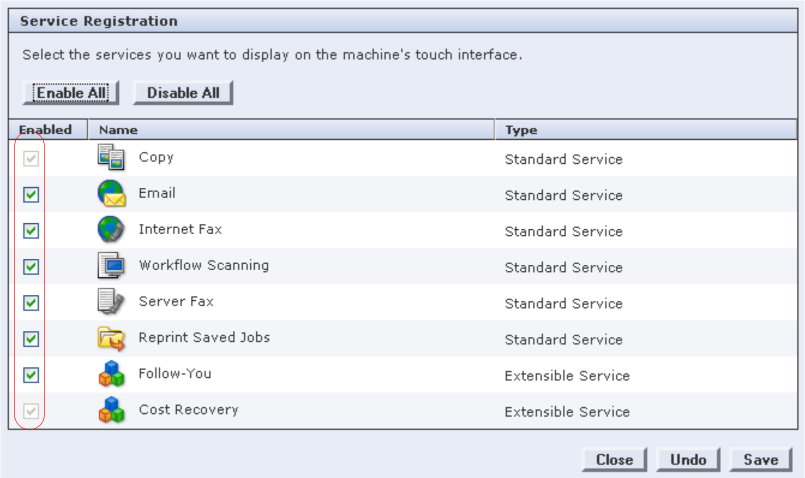
Note

The **Embedded** option must be **Enabled** on Xerox MFPs running EIP firmware version 1.5 or 2.0 in order for the attached card reader to operate normally.

b. In the **Device Log In Methods** section, select the preferred method.

c. In the **Accounting Information** section, select **Automatically apply Account Codes from the server**.

15. Click **Save** to apply the changes, then click **Close**.
16. Click **Close** again on the Xerox Secure Access Setup page to return to the main Authentication Configuration page.
17. Click the **Edit** button beside the **Service Registration** option.
18. Select the services you want users to access, then click **Save**.

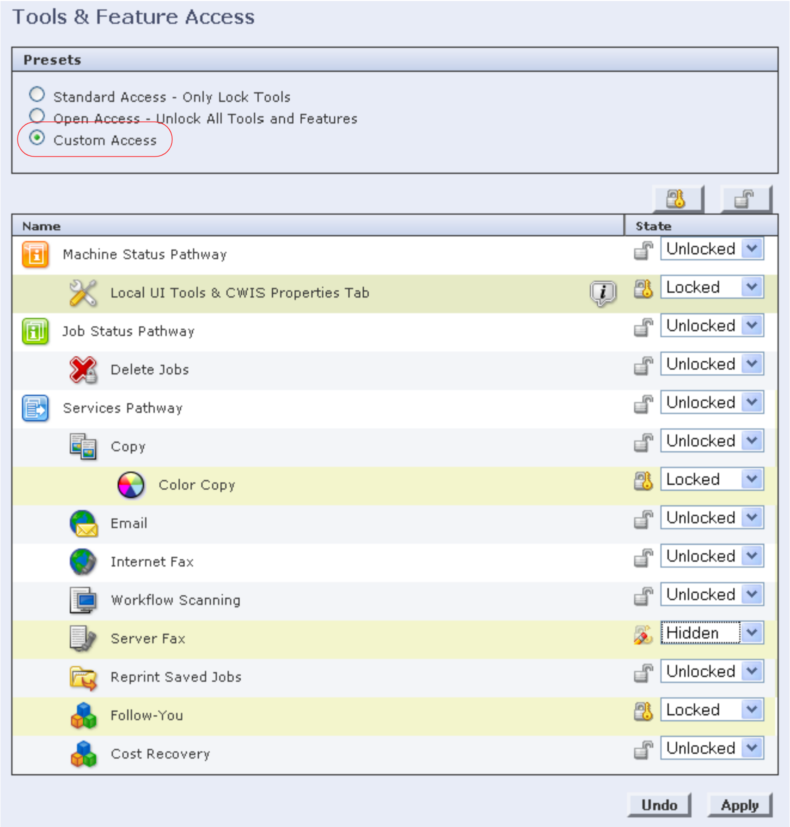


Service Registration

Select the services you want to display on the machine's touch interface.

Enabled	Name	Type
☑	Copy	Standard Service
☑	Email	Standard Service
☑	Internet Fax	Standard Service
☑	Workflow Scanning	Standard Service
☑	Server Fax	Standard Service
☑	Reprint Saved Jobs	Standard Service
☑	Follow-You	Extensible Service
☑	Cost Recovery	Extensible Service

19. In the left pane, click the **Security** folder, then the **Authentication** subfolder, and then **Tools & Feature Access**.



Tools & Feature Access

Presets

○ Standard Access - Only Lock Tools
○ Open Access - Unlock All Tools and Features
● Custom Access

Name	State
Machine Status Pathway	Unlocked
Local UI Tools & CWIS Properties Tab	Locked
Job Status Pathway	Unlocked
Delete Jobs	Unlocked
Services Pathway	Unlocked
Copy	Unlocked
Color Copy	Locked
Email	Unlocked
Internet Fax	Unlocked
Workflow Scanning	Unlocked
Server Fax	Hidden
Reprint Saved Jobs	Unlocked
Follow-You	Locked
Cost Recovery	Unlocked

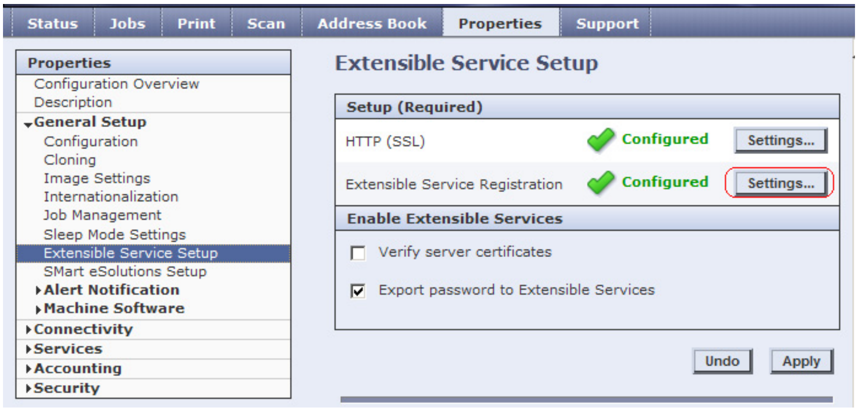
20. In the **Presets** section, select the **Custom Access** option to select the services you want to control access to.
    - Unlocked - the service appears on the control panel and is accessible without authentication.
    - **Locked** - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
    - **Hidden** - the service does not appear on the control panel.
21. Click **Apply** to complete the configuration of this MFP.
22. Logout of the MFP's configuration utility and close the web browser.

WorkCentre 76xx Series

You must configure the WorkCentre 76xx series from both the MFP Console and the Internet Services interface. Before starting the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **General Setup** folder, then select **Extensible Service Setup**.
4. Click the **Settings** button for the **Extensible Service Registration** setup option.



Extensible Service Setup

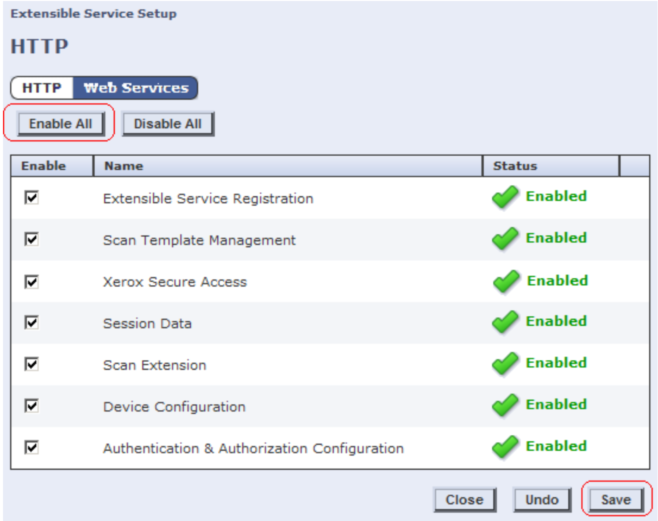
Setup (Required)		
HTTP (SSL)	✓ Configured	Settings...
Extensible Service Registration	✓ Configured	Settings...

Enable Extensible Services

☐ Verify server certificates

☑ Export password to Extensible Services

5. Click **Enable All,** then click **Save**. The Custom Services button should now be present on the MFP user interface when All Services is selected.



Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	Scan Template Management	✓ Enabled
☑	Xerox Secure Access	✓ Enabled
☑	Session Data	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	Device Configuration	✓ Enabled
☑	Authentication & Authorization Configuration	✓ Enabled

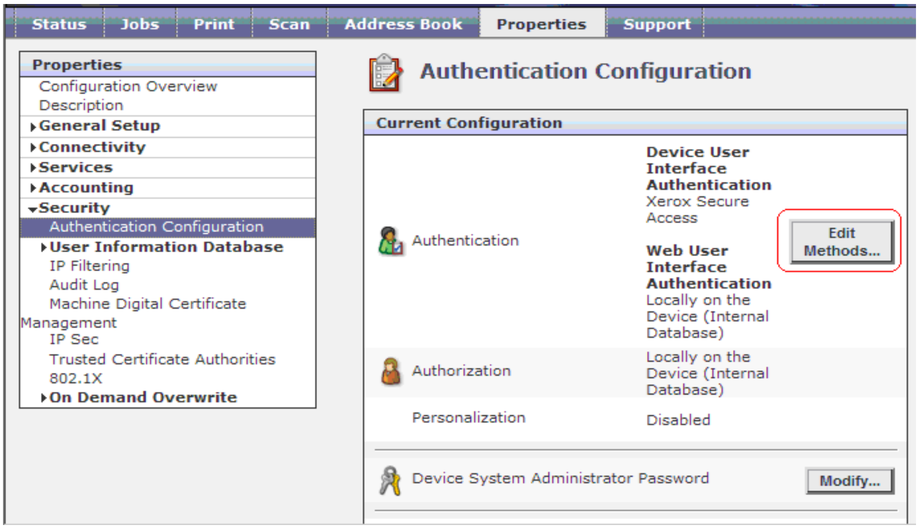
If you cannot access or locate these options, contact Xerox regarding correct installation of Custom Services.

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Enter the user name and password.
4. On the Machine Status screen, touch the Tools tab.
5. Touch **Accounting > Accounting Enablement > Accounting Mode**.
6. On the Accounting Mode screen, touch **Network Accounting**, then touch **Customize Prompts**.
7. On the Customize User Prompts screen, touch **Display Prompt 1 and 2,** then touch **Save** to save the changes. Failure to set this option causes transactions to be recorded against “Unidentified user”.
8. Touch the **Save** button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.

Via the Internet Services Interface

1. Open a Web browser and enter the URL `http://`**<MFP IP address>** in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **Security** folder, then select **Authentication Configuration**.
4. On the Authentication Configuration page, click **Edit Methods** to change the Authentication method.



Authentication Configuration

Current Configuration

Authentication — **Device User Interface Authentication** Xerox Secure Access; **Web User Interface Authentication** Locally on the Device (Internal Database)

Authorization — Locally on the Device (Internal Database)

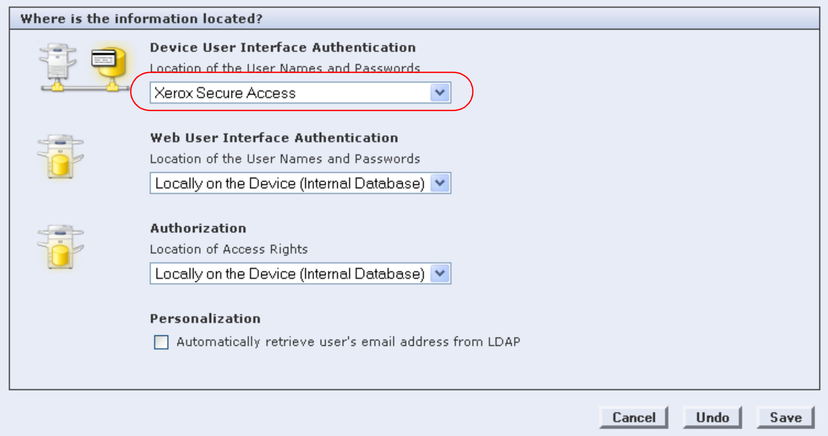
Personalization — Disabled

Device System Administrator Password

Note

If the copier has not been previously configured, you may need to click the **Next** button (instead of **Edit Methods)** and then work through a wizard to configure the copier.

5. Select **Xerox Secure Access** from the **Device User Interface Authentication** drop-down list. Leave both **Web User Interface Authentication** and **Authorization** options set to **Locally on the Device**.



Where is the information located?

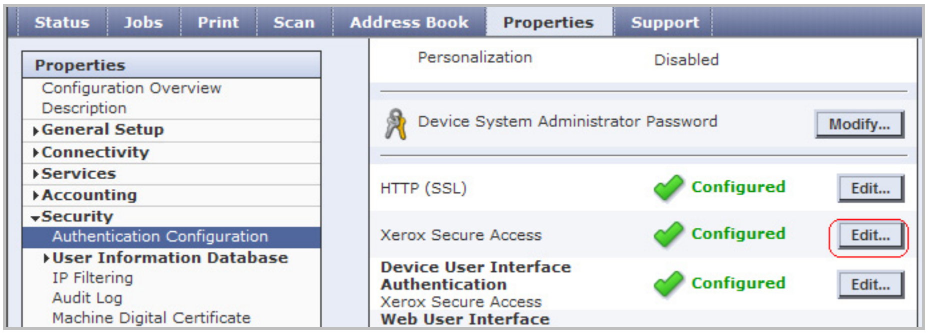
Device User Interface Authentication
Location of the User Names and Passwords
Xerox Secure Access

Web User Interface Authentication
Location of the User Names and Passwords
Locally on the Device (Internal Database)

Authorization
Location of Access Rights
Locally on the Device (Internal Database)

Personalization
□ Automatically retrieve user's email address from LDAP

6. Click **Save** to apply the changes.
7. On the Authentication Configuration page, click the **Edit** button beside the **Xerox Secure Access** option.

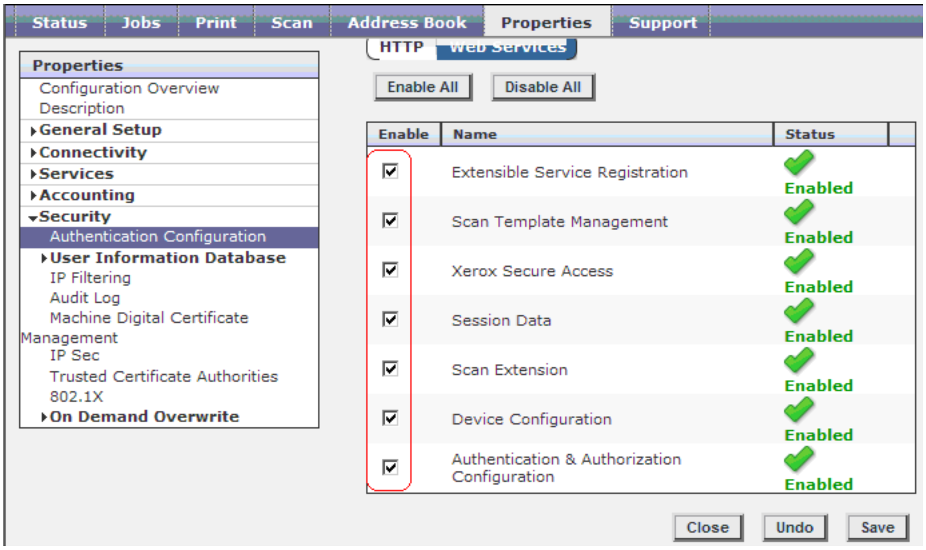


Personalization Disabled

Device System Administrator Password Modify...

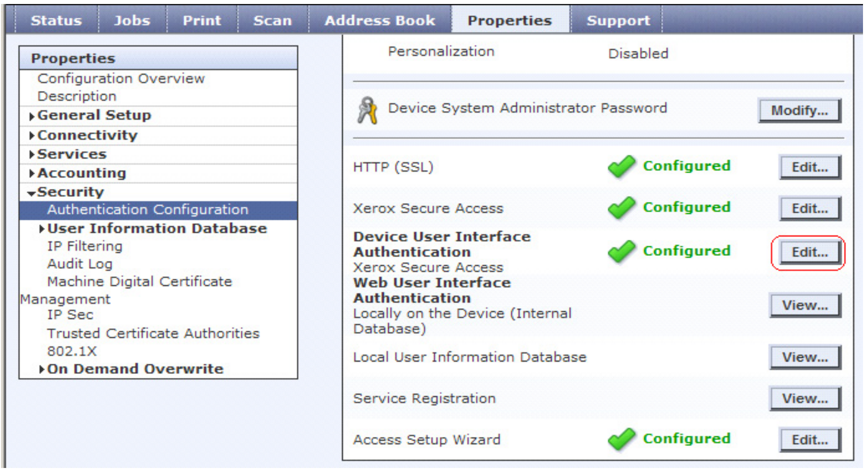
HTTP (SSL)	✓ Configured	Edit...
Xerox Secure Access	✓ Configured	Edit...
Device User Interface Authentication Xerox Secure Access	✓ Configured	Edit...
Web User Interface		

8. Ensure that all services listed are enabled, and then click save.



Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	Scan Template Management	✓ Enabled
☑	Xerox Secure Access	✓ Enabled
☑	Session Data	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	Device Configuration	✓ Enabled
☑	Authentication & Authorization Configuration	✓ Enabled

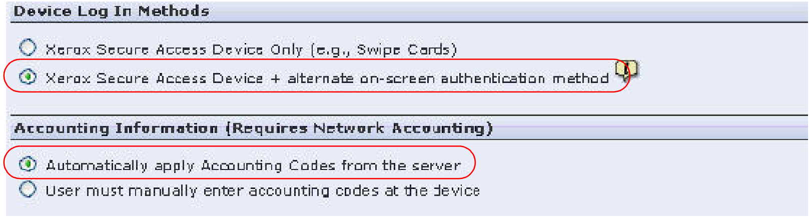
9. On the Authentication Configuration page, click the **Edit** button beside the **Device User Interface Authentication** option.



Personalization	Disabled	
Device System Administrator Password		Modify...
HTTP (SSL)	✓ Configured	Edit...
Xerox Secure Access	✓ Configured	Edit...
Device User Interface Authentication Xerox Secure Access	✓ Configured	Edit...
Web User Interface Authentication Locally on the Device (Internal Database)		View...
Local User Information Database		View...
Service Registration		View...
Access Setup Wizard	✓ Configured	Edit...

10. On the Xerox Secure Access Setup page, click the **Manually Override Settings** button.
11. Click **Manual Override Setting** at the bottom of the page.
12. On the Manual Override page, set the following:
    a. In the **Device Log In Methods** section, select the preferred method.
    - Xerox Secure Access Device Only – if you do not want people to use the alternate key board login button to enter their user ID
    - Xerox Secure Access Device + alternate on-screen authentication method – if you want people to also be able to use the alternate key board login button to enter their user ID

b. In the **Accounting Information** section, select **Automatically apply Account Codes from the server**.



Device Log In Methods

○ Xerox Secure Access Device Only (e.g., Swipe Cards)

● Xerox Secure Access Device + alternate on-screen authentication method

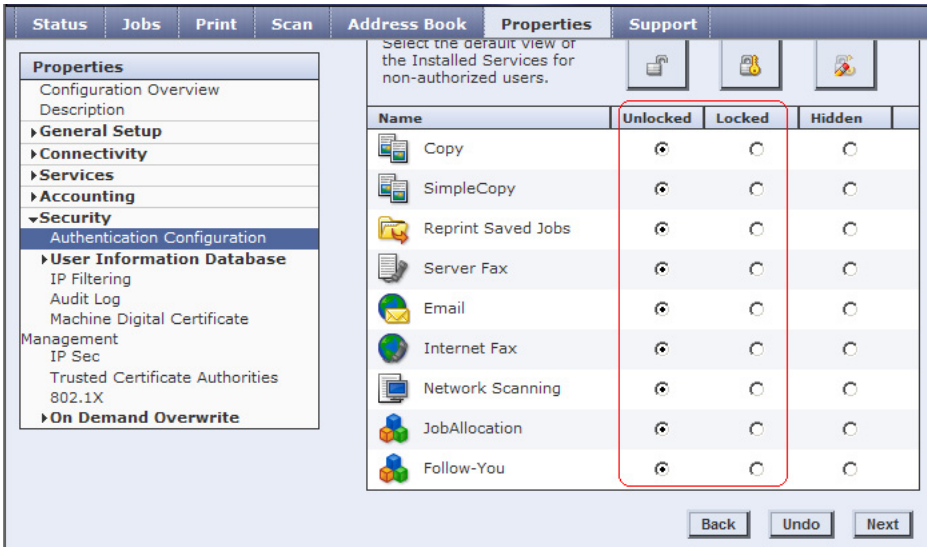
Accounting Information (Requires Network Accounting)

● Automatically apply Accounting Codes from the server

○ User must manually enter accounting codes at the device

13. Click **Save** to apply the changes, then click **Close**.
14. On the Authentication Configuration page, scroll down and click the **Edit** button beside the **Access Setup Wizard** option.
15. In the **Device Access** page, if you want to lock the front panel of the MFP, set the **Services Pathway** to **Locked** and then click **Save**, otherwise click the **Next** to continue.
16. To lock only certain features, leave Services Pathway set to **Unlocked** and click **Next**. Select the services you want to control access to, then click **Next**

- Unlocked - the service appears on the control panel and is accessible without authentication.
- **Locked** - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
- **Hidden** - the service does not appear on the control panel.



Select the default view of the Installed Services for non-authorized users.

Name	Unlocked	Locked	Hidden
Copy	●	○	○
SimpleCopy	●	○	○
Reprint Saved Jobs	●	○	○
Server Fax	●	○	○
Email	●	○	○
Internet Fax	●	○	○
Network Scanning	●	○	○
JobAllocation	●	○	○
Follow-You	●	○	○

17. Click **Finished** on the Feature Access page to complete the configuration of this MFP. The WorkCentre 76xx series device is now configured.
18. Logout of the MFP's configuration utility and close the web browser.

WorkCentre 77xx Series and ColorQube 93xx, 92xx or 89xx Series

You must configure the WorkCentre 77xx series MFP and the ColorQube 93xx, 92xx or 89xx Series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

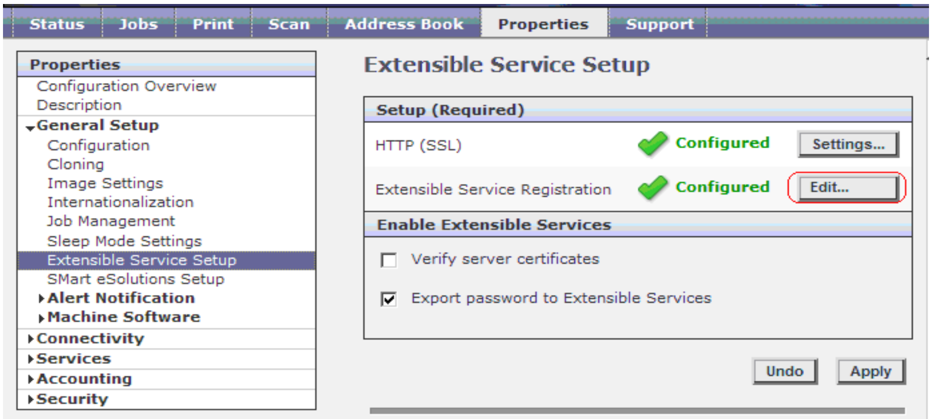
Note

This document assumes that any 89xx devices are running upgraded firmware that allows the device to function as a "ConnectKey" device. Devices with older firmware do not follow these instructions. For information about identifying which firmware version your device is running, see the Xerox support web site.

Locating Custom Services

Xerox EIP cannot be configured unless Custom Service is installed on the MFP. To determine if custom services is installed on a WorkCentre 77xx series and ColorQube 93xx, 92xx or 89xx Series, perform these steps:

1. Open a Web browser and enter the URL **http://<MFP IP address>** in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **General Setup** folder, then select **Extensible Service Setup**.
4. Click the **Edit** button beside the **Extensible Service Registration** option.



Extensible Service Setup

Setup (Required)

HTTP (SSL) ✓ Configured

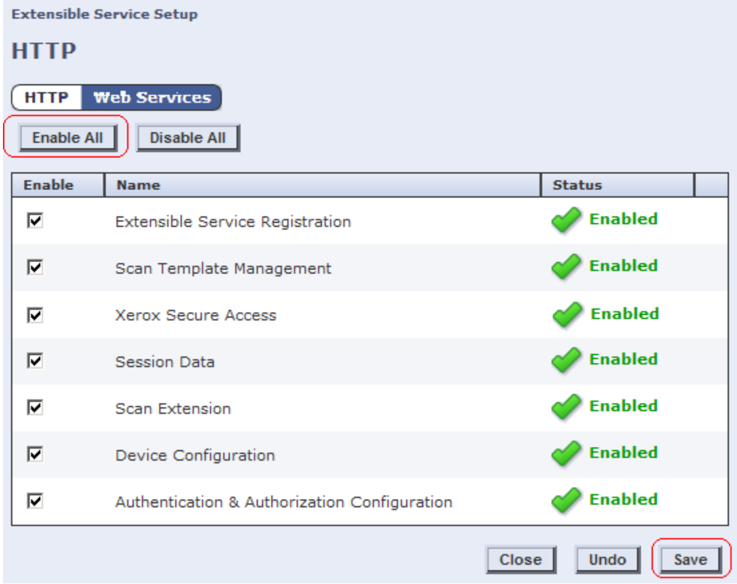
Extensible Service Registration ✓ Configured

Enable Extensible Services

☐ Verify server certificates

☑ Export password to Extensible Services

5. Click on **Enable All,** then click **Save**. The Custom Services button should now be present on the MFP user interface when All Services is selected.



Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	Scan Template Management	✓ Enabled
☑	Xerox Secure Access	✓ Enabled
☑	Session Data	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	Device Configuration	✓ Enabled
☑	Authentication & Authorization Configuration	✓ Enabled

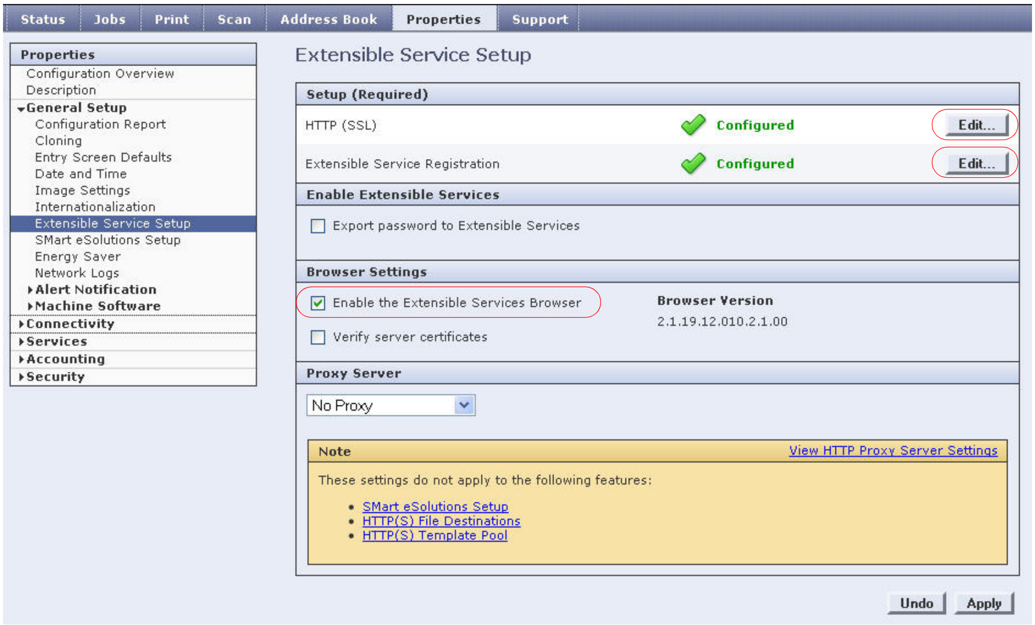
If you cannot access or locate these options, contact Xerox regarding correct installation of Custom Services.

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Enter the user name and password.
4. On the Machine Status screen, touch the **Tools** tab.
5. Touch **Accounting Settings > Accounting Mode**.
6. On the Accounting Mode screen, touch **Network Accounting**, then touch **Customize Prompts**.
7. On the Customize User Prompts screen, touch **Display Prompt 1 and 2,** then touch **Save**. Failure to set this option causes transactions to be recorded against “Unidentified user”.
8. Set **Code Entry Validation** to **Disabled**.
9. Touch the **Save** button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.

Via the Internet Services Interface

1. Open a Web browser and enter the URL **http://<MFP IP address>** in the Address field.
2. Select the **Properties** tab, and login with you User ID and Password when prompted.
3. In the left pane, click the **General Setup** folder, then select **Extensible Service Setup**.



Extensible Service Setup

Setup (Required)

HTTP (SSL) ✓ Configured

Extensible Service Registration ✓ Configured

Enable Extensible Services

□ Export password to Extensible Services

Browser Settings

☑ Enable the Extensible Services Browser

□ Verify server certificates

Browser Version
2.1.19.12.010.2.1.00

Proxy Server

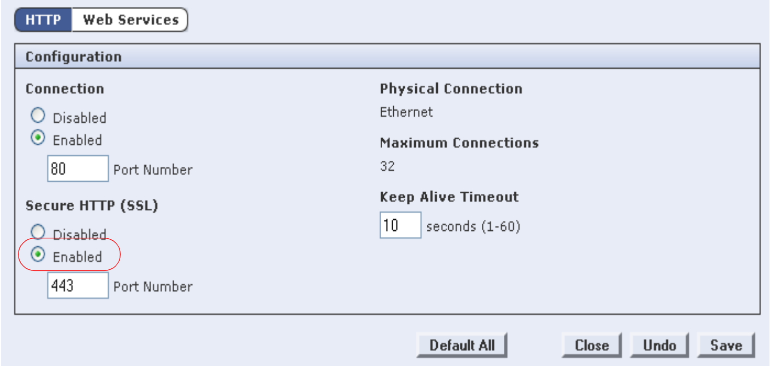
No Proxy

Note

These settings do not apply to the following features:

- SMart eSolutions Setup
- HTTP(S) File Destinations
- HTTP(S) Template Pool

4. Click the **Edit** button beside the **HTTP (SSL)** option.
5. Set the **Secure HTTP (SSL)** option to **Enabled,** then click **Save**.



Configuration

Connection
○ Disabled
● Enabled
80 Port Number

Secure HTTP (SSL)
○ Disabled
● Enabled
443 Port Number

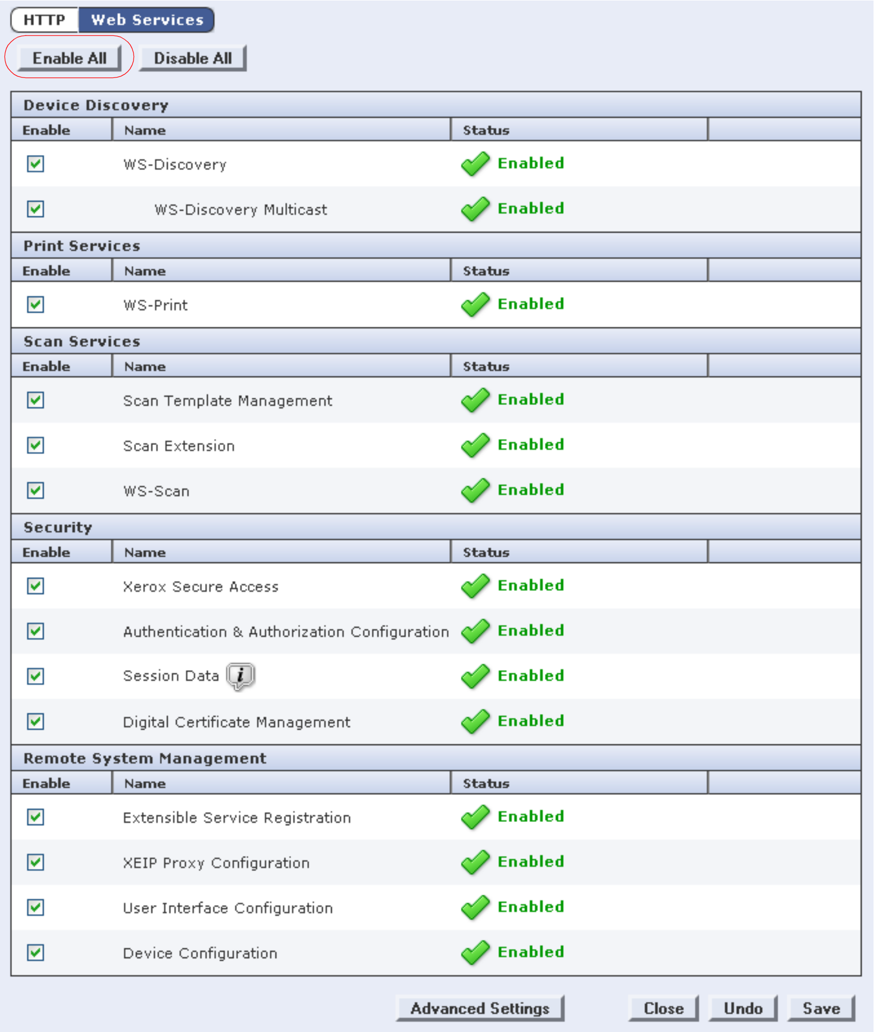
Physical Connection
Ethernet

Maximum Connections
32

Keep Alive Timeout
10 seconds (1-60)

6. Click the **Edit** button beside the **Extensible Service Registration** option.

7. Click **Enable All,** then click **Save**.



Device Discovery

Enable	Name	Status
☑	WS-Discovery	✓ Enabled
☑	WS-Discovery Multicast	✓ Enabled

Print Services

Enable	Name	Status
☑	WS-Print	✓ Enabled

Scan Services

Enable	Name	Status
☑	Scan Template Management	✓ Enabled
☑	Scan Extension	✓ Enabled
☑	WS-Scan	✓ Enabled

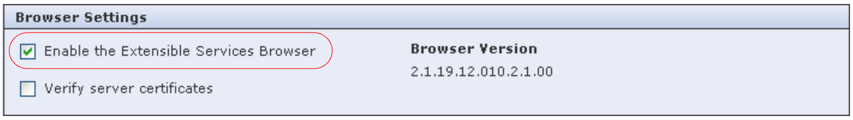
Security

Enable	Name	Status
☑	Xerox Secure Access	✓ Enabled
☑	Authentication & Authorization Configuration	✓ Enabled
☑	Session Data	✓ Enabled
☑	Digital Certificate Management	✓ Enabled

Remote System Management

Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	XEIP Proxy Configuration	✓ Enabled
☑	User Interface Configuration	✓ Enabled
☑	Device Configuration	✓ Enabled

8. In the **Browser Settings** section on the Extensible Service Setup page, select the **Enable the Extensible Services Browser** checkbox. and click **Apply**.



Browser Settings

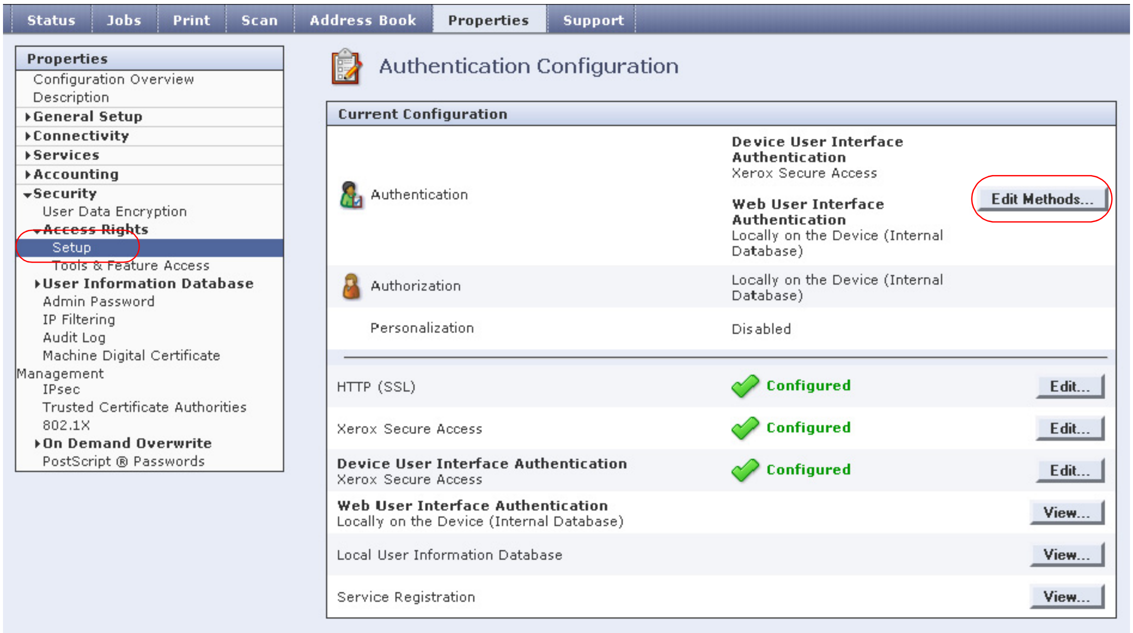
☑ Enable the Extensible Services Browser

□ Verify server certificates

Browser Version
2.1.19.12.010.2.1.00

9. In the left pane, click the **Security** folder, then the **Access Rights** subfolder, and then **Setup**.

10. In the right pane, click **Edit Methods** to change the Authentication method.



Status | Jobs | Print | Scan | Address Book | Properties | Support

Properties
Configuration Overview
Description
General Setup
Connectivity
Services
Accounting
Security
User Data Encryption
Access Rights
Setup
Tools & Feature Access
User Information Database
Admin Password
IP Filtering
Audit Log
Machine Digital Certificate Management
IPsec
Trusted Certificate Authorities
802.1X
On Demand Overwrite
PostScript ® Passwords

Authentication Configuration

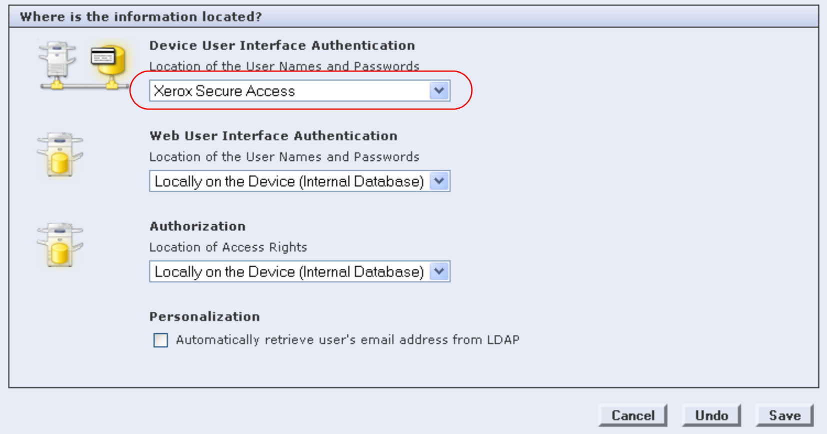
Current Configuration

Authentication	**Device User Interface Authentication** Xerox Secure Access **Web User Interface Authentication** Locally on the Device (Internal Database)	Edit Methods...
Authorization	Locally on the Device (Internal Database)	
Personalization	Disabled	
HTTP (SSL)	✓ Configured	Edit...
Xerox Secure Access	✓ Configured	Edit...
Device User Interface Authentication Xerox Secure Access	✓ Configured	Edit...
Web User Interface Authentication Locally on the Device (Internal Database)		View...
Local User Information Database		View...
Service Registration		View...

Note

If the copier has not been previously configured, you may need to click the **Next** button (instead of *E***dit Methods)** and then work through a wizard to configure the copier.

11. Select **Xerox Secure Access** from the **Device User Interface Authentication** drop-down list. Leave both **Web User Interface Authentication** and **Authorization** options set to **Locally on the Device**.



Where is the information located?

Device User Interface Authentication
Location of the User Names and Passwords
Xerox Secure Access

Web User Interface Authentication
Location of the User Names and Passwords
Locally on the Device (Internal Database)

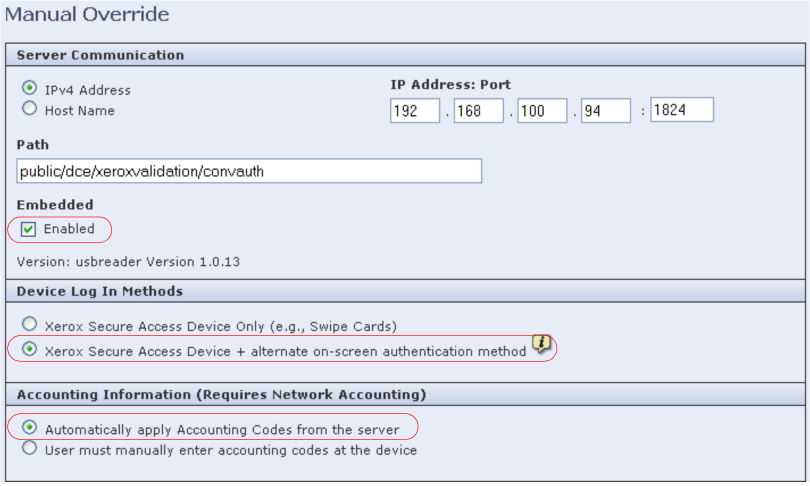
Authorization
Location of Access Rights
Locally on the Device (Internal Database)

Personalization
□ Automatically retrieve user's email address from LDAP

Cancel | Undo | Save

12. Click **Save** to apply the changes.
13. On the Authentication Configuration page, click the **Edit** button beside the **Device User Interface Authentication** option.
14. On the Xerox Secure Access Setup page, click the **Manually Override Settings** button.
15. On the Manual Override page, set the following:
    a. In the **Server Communication** section, set the **Embedded** option to **Enabled**.
    b. In the **Device Log In Methods** section, select the preferred method.

c. In the **Accounting Information** section, select **Automatically apply Account Codes from the server**.



Manual Override

Server Communication

● IPv4 Address
○ Host Name

IP Address: Port
192 . 168 . 100 . 94 : 1824

Path
public/dce/xeroxvalidation/convauth

Embedded
☑ Enabled

Version: usbreader Version 1.0.13

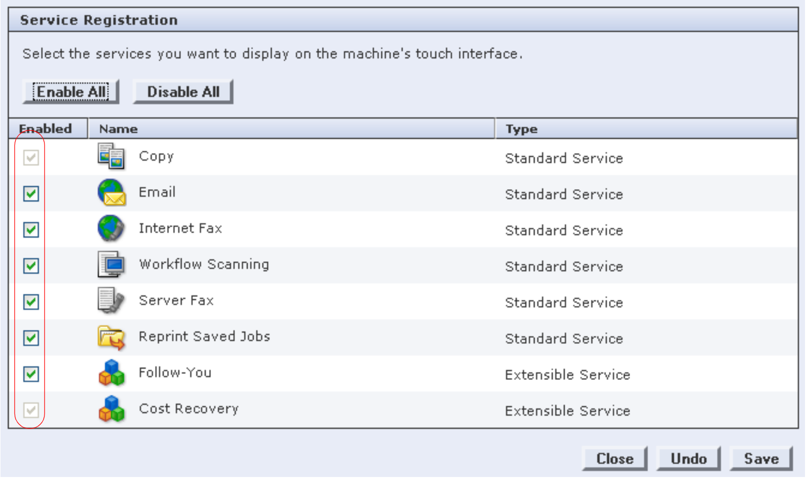
Device Log In Methods

○ Xerox Secure Access Device Only (e.g., Swipe Cards)
● Xerox Secure Access Device + alternate on-screen authentication method

Accounting Information (Requires Network Accounting)

● Automatically apply Accounting Codes from the server
○ User must manually enter accounting codes at the device

16. Click **Save** to apply the changes, then click **Close**.
17. Click **Close** again on the Xerox Secure Access Setup page to return to the main Authentication Configuration page.
18. Click the **View** button beside the **Service Registration** option.
19. Select the services you want users to access, then click **Save**.

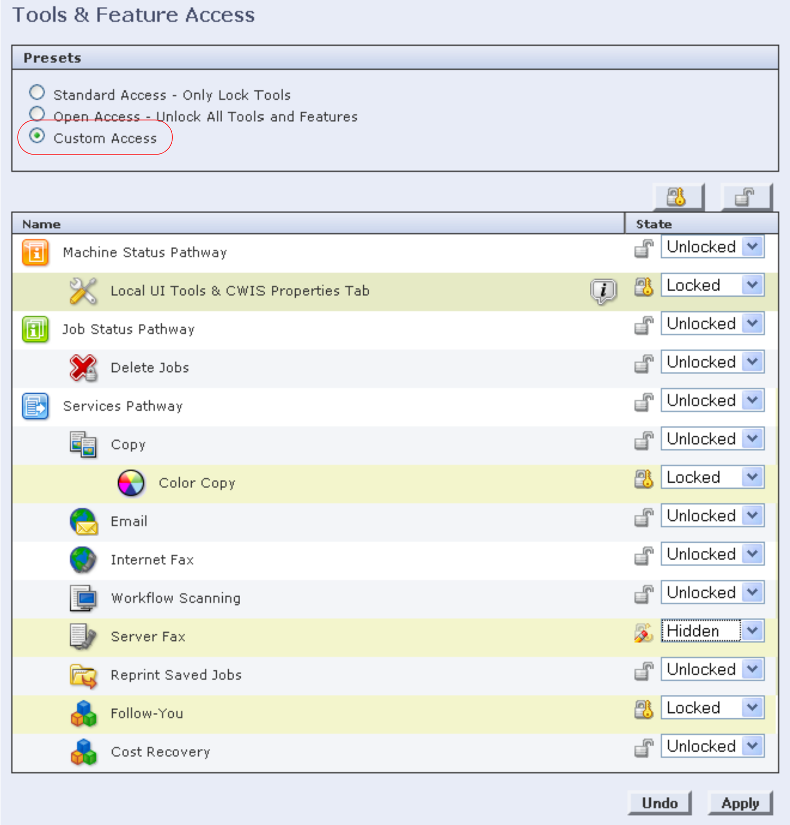


Service Registration

Select the services you want to display on the machine's touch interface.

Enabled	Name	Type
☑	Copy	Standard Service
☑	Email	Standard Service
☑	Internet Fax	Standard Service
☑	Workflow Scanning	Standard Service
☑	Server Fax	Standard Service
☑	Reprint Saved Jobs	Standard Service
☑	Follow-You	Extensible Service
☑	Cost Recovery	Extensible Service

20. In the left pane, click the **Security** folder, then the **Access Rights** subfolder, and then **Tools & Feature Access**.



Tools & Feature Access

Presets

○ Standard Access - Only Lock Tools
○ Open Access - Unlock All Tools and Features
● Custom Access

Name	State
Machine Status Pathway	Unlocked
Local UI Tools & CWIS Properties Tab	Locked
Job Status Pathway	Unlocked
Delete Jobs	Unlocked
Services Pathway	Unlocked
Copy	Unlocked
Color Copy	Locked
Email	Unlocked
Internet Fax	Unlocked
Workflow Scanning	Unlocked
Server Fax	Hidden
Reprint Saved Jobs	Unlocked
Follow-You	Locked
Cost Recovery	Unlocked

21. In the **Presets** section, select the **Custom Access** option to select the services you want to control access to.
    - Unlocked - the service appears on the control panel and is accessible without authentication.
    - **Locked** - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
    - **Hidden** - the service does not appear on the control panel.
22. Click **Apply** to complete the configuration of this MFP.
23. Logout of the MFP's configuration utility and close the web browser.

WorkCentre Pro 2xx Series

You must configure the WorkCentre Pro 2xx series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. Select the **Services** folder in the left navigation pane, then select the **Custom Services** subfolder. If there is another sub-option in this folder called **Custom Services**, then the service is installed and you can proceed.

   Note

   If the services are not installed, contact Xerox regarding correct installation of these services.

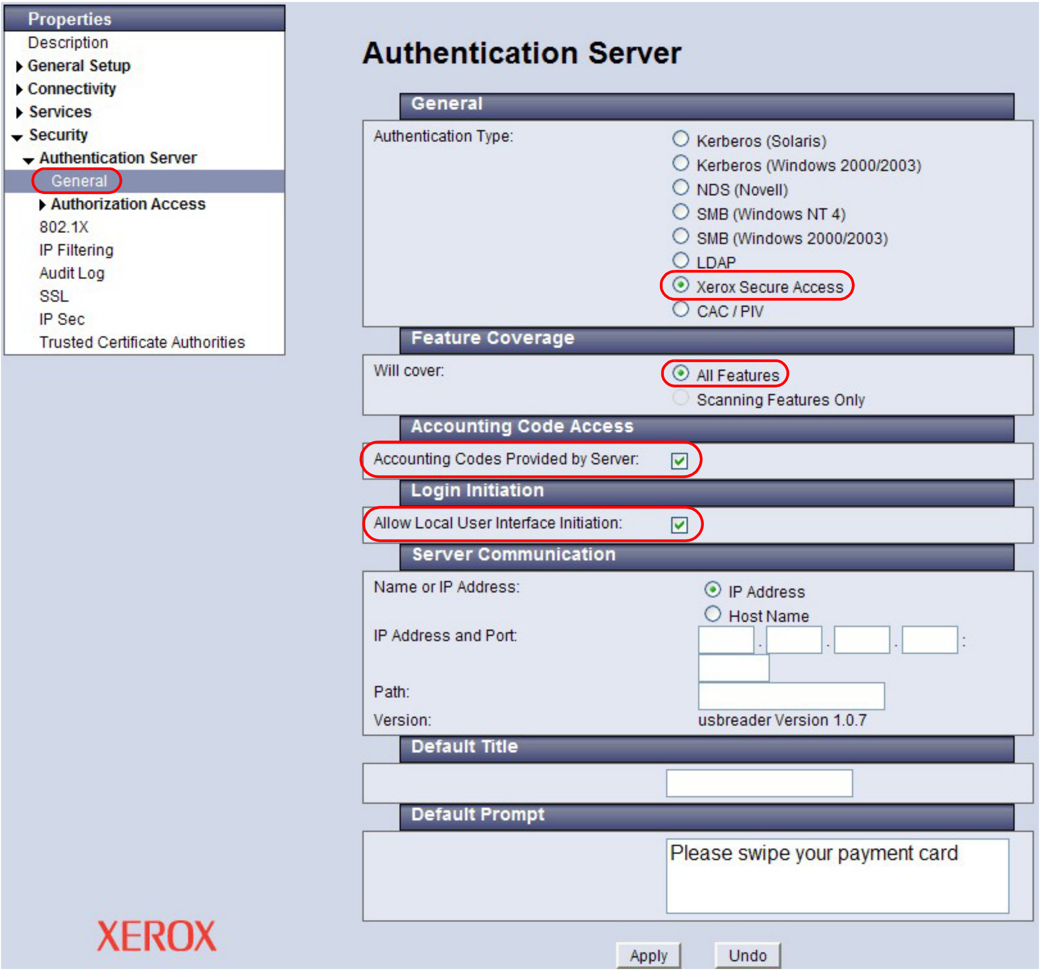
4. In the right pane, ensure that **Custom Services** is set to **Enabled**, then click **Apply**. The Custom Services button should now be present on the MFP user interface when All Services is selected.

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Touch **Access and Accounting**.
4. Touch **Authentication Mode**.
5. Under Network Accounting, touch the **On** option to enable Network Accounting. Ensure that all other authentication options are disabled. Touch **Save**.
6. Return to the **Access and Accounting** menu, then touch **Network Accounting Setup**.
7. Touch **Network Accounting Authentication**.
8. Exit the Tools screen, and return to copy mode. Configuration on the MFP is now complete.

Via the Internet Services Interface

1. Open a web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **Security** folder, then the **Authentication Server** subfolder, and the **General**.



Authentication Server

General

Authentication Type: ○ Kerberos (Solaris) ○ Kerberos (Windows 2000/2003) ○ NDS (Novell) ○ SMB (Windows NT 4) ○ SMB (Windows 2000/2003) ○ LDAP ● Xerox Secure Access ○ CAC / PIV

Feature Coverage

Will cover: ● All Features ○ Scanning Features Only

Accounting Code Access

Accounting Codes Provided by Server: ☑

Login Initiation

Allow Local User Interface Initiation: ☑

Server Communication

Name or IP Address: ● IP Address ○ Host Name

IP Address and Port:

Path:

Version: usbreader Version 1.0.7

Default Title

Default Prompt

Please swipe your payment card

4. In the right pane, set the following options:
   a. In the **General** section, set the **Authentication Type** to **Xerox Secure Access**.
   b. In **Feature Coverage**, select **All Features**.
   c. In **Account Codes Access**, enable the **Accounting Codes Provided by Server** option.
   d. In **Login Initiation**, enable the **Allow Local User Interface Initiation** option to make the keyboard access button visible. This is optional.
   e. In **Server Communication**, leave the fields blank. The Xerox Secure Access server will complete this information when you Initialize this MFP later on in the workflow.
5. Click **Apply** to complete the configuration of this MFP.
6. Logout of the MFP's configuration utility and close the web browser.

Phaser 3635

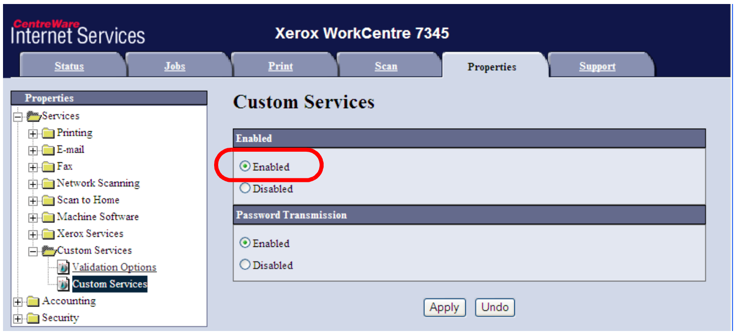
Configuration of Phaser 36xx MFPs is performed in two steps: First, via the Internet Services interface, and then at the MFP to select Xerox ECSP as the default application.

Caution

In order to enable Network Authentication, a default "From" address must be configured. If you have not yet done so, designate an email address by navigating to **Services > E-mail Settings > Defaults**. Under the **General** section, click the **Edit** button, and type a default From email address in the **From address** field, then click **Apply**.

Internet Services Interface Configuration

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **Services > Custom Services**. The **Custom Services** screen displays:



Custom Services

Enabled

● Enabled
○ Disabled

Password Transmission

● Enabled
○ Disabled

Apply Undo

4. Ensure that **Custom Services** is set to **Enabled**, then click **Apply**. The **Custom Services** button should now be present on the MFP user interface when **All Services** is selected.

   Note

   Select this option only if you want to enable keyboard access to the device for login purposes. With this option deselected, only card swipe login is possible.

   a. The settings in the **Server Communication** section are populated from settings determined when the embedded device was set up.
   b. Provide a **Default Title** and **Default Prompt** the user sees when starting to use the device.
   c. The **Logoff Reminder** is selected by default, and cannot be altered.
5. Click **Apply**.

Phaser MFP Configuration

Phaser MFPs require that you set the device default application manually. By setting this, the device uses the Xerox ECSP by default.

For each Phaser MFP using Xerox ECSP, go to the device, and do the following:

1. Press the **Machine Status** hard key to the left of the display.
2. Touch the **Guest** button at the top right of the display, then select **Log In** from the drop-down menu.
3. Touch the Keyboard icon in the center of the screen, and using the soft keyboard, provide your administrator password to log in to the device. The System Administration screen displays:
4. Select the **Tools** tab, then select **User Interface**, and **General**. The **User Interface General** settings options display.

5. From the list of features, select **Screen Defaults**.

   a. Select **Entry Screen Default**

   b. Select **Features**

   c. Select **Save**

   d. Select **Default Feature and Priority Order**

6. Set the **Highest Priority** service:

   a. From the list of priorities, touch the **Custom Services...** button to select it.

   Note

   If the **Custom Services...** option is absent from the list, return to the **Entry Screen Default** list, deselect **Features** and then reselect **Features**. This resets the **Highest Priority** list.

   b. Use the arrow buttons to the right of the list to move the **Custom Services...** button to the top of the list.

   Note

   The **Highest Priority** list can only display 4 options. If your option is not listed, move one of the listed options to the bottom of the list.

7. From the **EIP app list**, touch **Xerox ECSP** to select it.

8. Touch **Save.**

9. Touch **Close.**

10. Touch the **Admin** button at the top right of the display, then select **Log Out**.

Caution

If a device is initialized to point to a different DWS server after initial setup, the default Highest Priority service must be manually reset to prevent ECSP from inappropriately displaying the login screen. To reset the Highest Priority service follow steps 6. through 8. above, selecting **Custom Services** from **EIP app list**, and then follow these steps a second time, reselecting **Xerox ECSP** as the Highest Priority service.

Other settings

1. In the left pane, select the **Security > Authentication > Authentication**. The **Authentication** screen displays:

   a. Ensure in the **Guest Access** section, **Allow Guess Access** is **deselected**.

   b. Ensure in the **Feature Coverage** section, **All Features** is **selected**.

   c. Ensure **Accounting Code Access** is **Enabled**.

   d. In the **Login Initiation** section, deselect **Allow Local User Interface Initiation**.

Smart Card Configuration

The Xerox Smart Card solution provides a two-factor identification requirement. Users must insert their access card and enter a unique PIN at the device. Once validated, a user is logged into the Xerox device for all features.

The Smart Card solution requires a Smart Card Enablement Kit and a Feature Enable Key, provided by Xerox.

Before installing the Xerox Smart Card solution, the software needs to be enabled on both the MFP Console and via the Internet Services interface.

On the MFP Console

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **More** to access additional Tools options.
3. Touch **Optional Services**. If necessary, use More to navigate to the option.
4. Touch **Smart Card**. If necessary, use More to navigate to the option.
5. When prompted, touch the **Option Kit Number** entry field and enter the unique **Feature Enable Key** provided with the Smart Card Enablement kit.
6. Touch **Exit Tools**.
7. Reboot the device. The device may automatically reboot.

Once the reboot is complete, the Smart Card function is ready to be configured using the Internet Services interface.

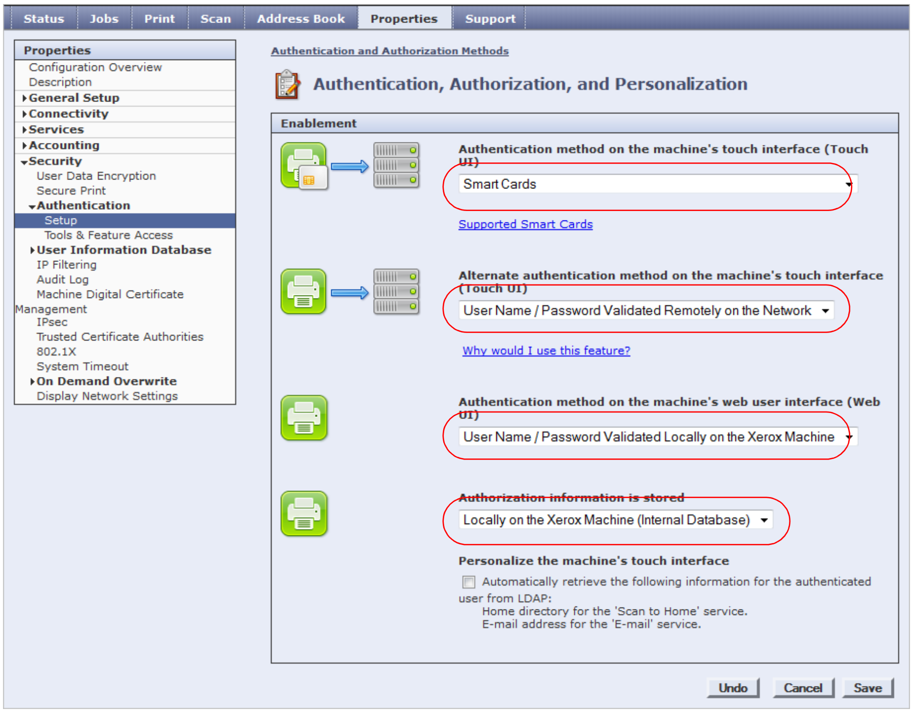
Note

No services on the device will be restricted until Smart Card has been configured using Internet Services.Via the Internet Services Interface

Via the Internet Services Interface

To enable and configure the Smart Card, do the following:

1. Open a Web browser and enter the URL **http://<MFP IP address>** in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **Security** folder, then the **Authentication** subfolder, and then **Setup.**
4. On the Xerox Access Setup page, click the **Edit** button to change the Authentication method.
5. On the Authentication, Authorization and Personalization page, do the following:



Authentication, Authorization, and Personalization

Enablement

Authentication method on the machine's touch interface (Touch UI): Smart Cards

Alternate authentication method on the machine's touch interface (Touch UI): User Name / Password Validated Remotely on the Network

Authentication method on the machine's web user interface (Web UI): User Name / Password Validated Locally on the Xerox Machine

Authorization information is stored: Locally on the Xerox Machine (Internal Database)

Personalize the machine's touch interface

☐ Automatically retrieve the following information for the authenticated user from LDAP:
Home directory for the 'Scan to Home' service.
E-mail address for the 'E-mail' service.

a. Select **SmartCards** from the **Authentication method on the machine's touch interface** drop-down list.

b. Select **User Name/Password Validated Remotely on the Network** from the **Alternate authentication method on the machine's touch interface (Touch UI)** drop-down list.

c. Select **User Name/Password Validated Locally on the Xerox Machine** from the **Authentication method on the machine's web user interface (Web UI)** drop-down list.

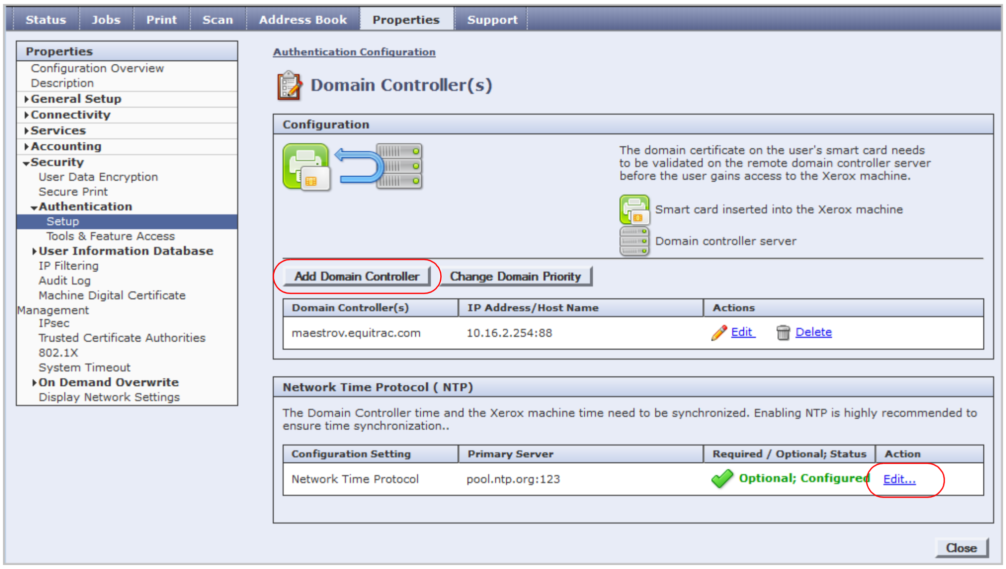
d. Select **Locally on the Xerox Machine (Internal Database)** from the **Authorization information is stored** drop-down list.

e. Click **Save** to apply the changes.

A list of configuration settings appears at the bottom of the Xerox Access Setup page. Click **Edit** to configure any settings that are marked in red text as **Required; Not Configured**.

Configuring Domain Controller Settings

1. In the **Configuration Settings** table on the Xerox Access Setup page, click **Edit** on the **Domain Controller(s)** row. The domain certificate on a user's Smart Card must be validated on the domain controller server before they can access the MFP.



Domain Controller(s)

Configuration

The domain certificate on the user's smart card needs to be validated on the remote domain controller server before the user gains access to the Xerox machine.

Smart card inserted into the Xerox machine

Domain controller server

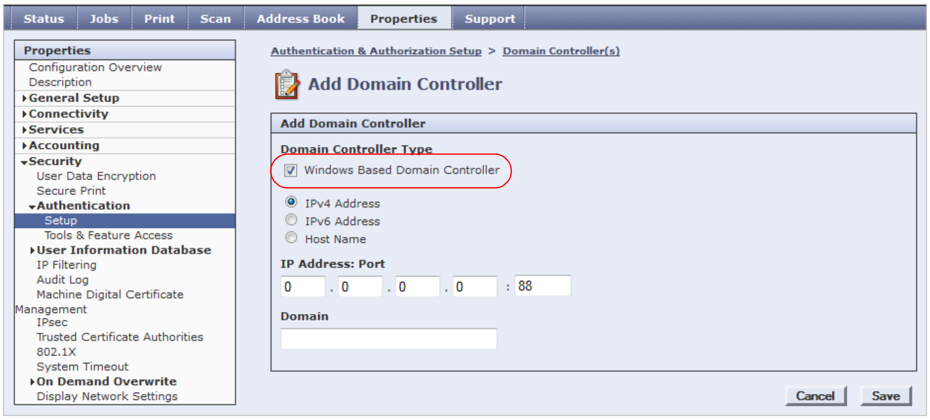
Domain Controller(s)	IP Address/Host Name	Actions
maestrov.equitrac.com	10.16.2.254:88	Edit Delete

Network Time Protocol (NTP)

The Domain Controller time and the Xerox machine time need to be synchronized. Enabling NTP is highly recommended to ensure time synchronization..

Configuration Setting	Primary Server	Required / Optional; Status	Action
Network Time Protocol	pool.ntp.org:123	✓ Optional; Configured	Edit...

2. Click **Add Domain Controller**.



Add Domain Controller

Add Domain Controller

Domain Controller Type

☑ Windows Based Domain Controller

● IPv4 Address
○ IPv6 Address
○ Host Name

IP Address: Port

0 . 0 . 0 . 0 : 88

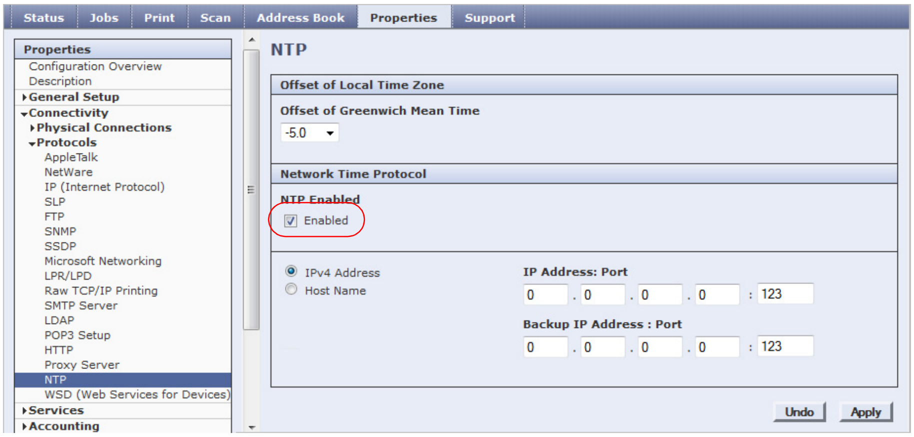
Domain

3. Under **Domain Controller Type**, select **Windows Based Domain Controller**.
4. Select the **IPv4** option and enter the domain controller server **IP Address** and **Port** number.
5. Enter the **Domain** name.
6. Click **Save** to apply the new settings and return to the Domain Controller page.

Note

If you have more that one domain controller server, you can click **Change Domain Priority** and use the Up and Down arrows to change the search priority of the server.

7. Click **Edit** beside **Network Time Protocol** (NTP).



NTP

Offset of Local Time Zone

Offset of Greenwich Mean Time: -5.0

Network Time Protocol

NTP Enabled: ☑ Enabled

● IPv4 Address
○ Host Name

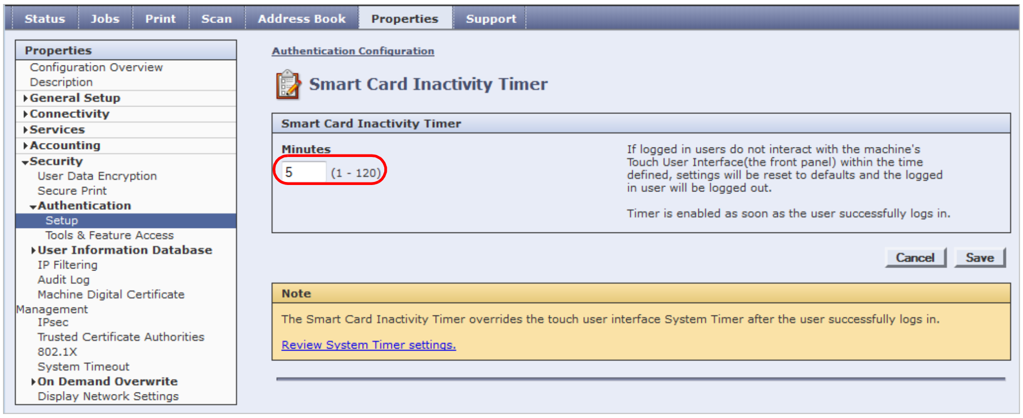
IP Address: Port: 0 . 0 . 0 . 0 : 123

Backup IP Address : Port: 0 . 0 . 0 . 0 : 123

8. Enable **NTP** to ensure time synchronization between the domain controller and the MFP.
9. Click **Close** to return to the Xerox Access Setup page.

Setting the Inactive Time Limit

1. In the **Configuration Settings** table on the Xerox Access Setup page, click **Edit** on the **Smart Card Inactivity Timer** row.



Smart Card Inactivity Timer

Smart Card Inactivity Timer

Minutes: 5 (1 - 120)

If logged in users do not interact with the machine's Touch User Interface(the front panel) within the time defined, settings will be reset to defaults and the logged in user will be logged out.

Timer is enabled as soon as the user successfully logs in.

Note

The Smart Card Inactivity Timer overrides the touch user interface System Timer after the user successfully logs in.

2. Specify the maximum amount of Smart Card inactivity time (in minutes) before a user is automatically logged out.
3. Click **Save** to apply the new settings and return to the Authentication Setup page.

The Smart Card settings are now configured. Please refer to the Xerox *Smart Card Installation Guide* to install the Smart Card hardware.

3

Server-Side Configuration

Topics

To enable Xerox Secure Access, you must configure the Authentication Devices, MFPs, and the core accounting server (CAS). Follow the steps below in the order they are presented to ensure a successful install.

Licensing Embedded Devices

The Xerox Secure Access system utilizes a 6 tier licensing structure which allows licenses to be assigned on a per device basis. The license tiers are as follows:

Authentication – Any time the user approaches a device and authenticates themselves, they are using an Authentication license. This could be for a PageCounter, ID Controller, Web Release or Embedded device. Desktop Printing is not considered authentication.

- Licenses are assigned per device where authentication is required.
- Does not require a prerequisite.

Follow-You Printing® – Allows the user the ability to release a job from a device with this license assigned to it. Includes Web Release, PageCounter, Embedded and ID Controller.

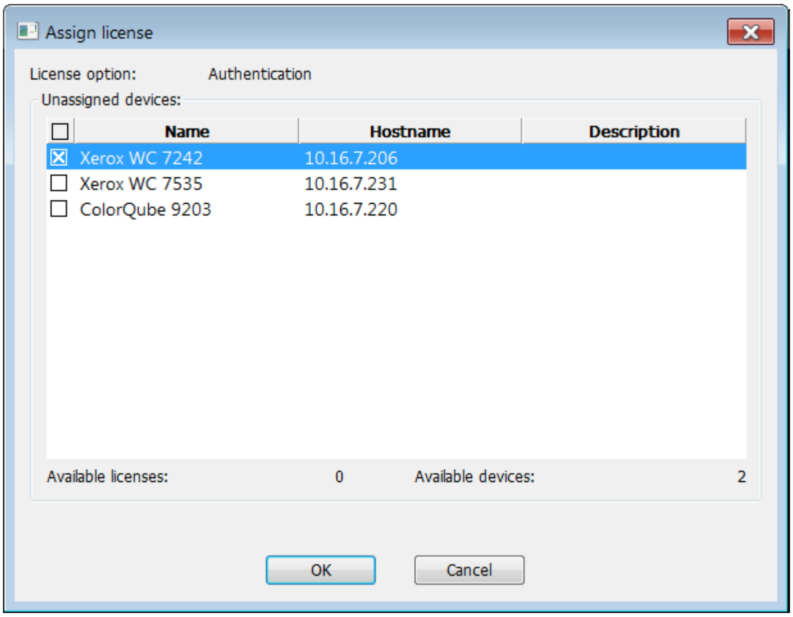
- License are assigned per device where Follow-You Printing is required.
- Requires an Authentication license as a prerequisite.

Assigning Licenses to Devices

Licenses must be assigned to each printer that will use that particular feature.

To assign a license, do the following:

1. Open **System Manager**, and select **Licensing** in the left pane.
2. Select the **Assignment View tab to open the** list of all assigned licenses.
3. Expand or right-click the desired license option, and select **Add** to open the **Assign license** dialog box.



License option: Authentication

Unassigned devices:

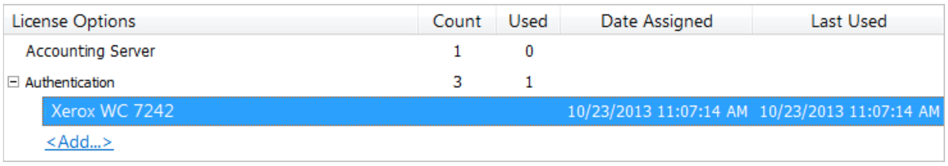
□	Name	Hostname	Description
☒	Xerox WC 7242	10.16.7.206	
□	Xerox WC 7535	10.16.7.231	
□	ColorQube 9203	10.16.7.220	

Available licenses: 0 Available devices: 2

4. On the **Assign license** dialog box, select the checkbox for the device(s) to assign the license to.

   At the bottom of the dialog box is a counter displaying the number of available licenses and available devices. These numbers decrease with every license assigned.
5. Click **OK** after the licenses have been assigned to the desired devices.

The devices assigned to the license now display under the selected license option.



License Options	Count	Used	Date Assigned	Last Used
Accounting Server	1	0		
⊟ Authentication	3	1		
Xerox WC 7242			10/23/2013 11:07:14 AM	10/23/2013 11:07:14 AM
<Add...>				

To remove an assigned license from a device, right-click the device and select **Remove assignment**. The number of used licenses will be adjusted accordingly.

Configuring Printer Ports

Controlled Xerox MFPs must use an Equitrac® Port (rather than standard TCP/IP ports) to enable secure printing. If you are configuring a secure print environment, ensure that your devices comply with this requirement.

You can create Equitrac printer ports directly for new devices, or convert existing devices from standard TCP/IP ports into Equitrac ports. For new devices, see Add a Printer on an Equitrac Printer Port (below). Alternatively, new devices can be created using standard TCP/IP ports and then converted it to an Equitrac ports. For existing devices, see Convert an Existing TCP/IP Port to Equitrac Port on page 5. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports to determine if reported errors within the print environment are due to the Xerox Secure Access server or the normal print environment.

Add a Printer on an Equitrac Printer Port

To create Equitrac printer ports for new devices, do the following:

1. Using the standard Windows interface, open the **Add Printer** wizard.
2. Follow the prompts to **add a local printer** and create a new port.
3. Select **Equitrac Port** as the type of port you want to create and click **Next**.
4. The Add Equitrac Printer Port wizard displays and you are prompted to ensure that the printer device is turned on, connected to the network, and properly configured. Click **Next** to continue.
5. Click **Next** and select **Physical printer** as your **Device Type** from the drop-down list.
6. Specify a **Printer name** or **IP Address**. The wizard supplies a Port name prefaced with *"EQ_ "*based on the printer name or IP address. If another naming convention is preferred, rename the port accordingly.
7. Click **Next** to continue with the port configuration options. The Port Configuration screen displays. The **Detected device information** displays automatically if the wizard is able to collect this data from the printer.
8. Select the **Use custom settings** option:
   - If you select **Raw port** communication, identify the TCP **Port** number, and specify if the port monitor should hold the connection open.
   - If you select **LPR**, specify the name of the print **Queue** on the physical device (e.g. PORT1).
   - If you select **Specific device**, select the appropriate **Manufacturer** and **Model** from the drop-down lists. The device uses the relevant default communications parameters based on these selections.
9. Click **Next** and specify the **Physical device name**. This is the name of the device that is displayed within System Manager.
10. Review the details for this new port and device registration, and click **Finish** to close the Add Equitrac Printer Port wizard, or **Back** to change any of the settings.
11. Specify the Manufacture and model to install the printer driver, and click **Next**.

Note

If the device is part of a pull group, it must use the same drivers as all other devices in the pull group. You must select the model of the pull group driver, not the model of the device. If the DRE is a 64-bit server you must also load the 32-bit driver to the server.

12. Specify the version of the print driver to use, and click **Next**.
13. Enter the **Printer name**, and click **Next**. This is the name of the device that is displayed in System Manager.
14. Select to share or not to share the printer with others, and click **Next**. If sharing the printer, enter a Share name, and optionally provide a printer location and any comments.
15. Click the **Print a test page** button, and click **Finish** to close the Add Printer wizard.
16. Confirm that the test page printed successfully.
17. Verify that the physical device and its printer port and print queue appear in **System Manager > Devices**.

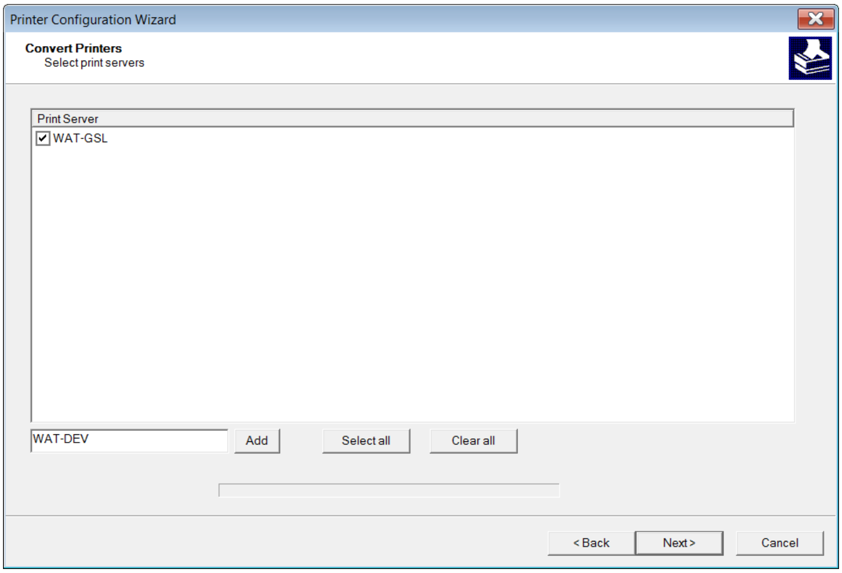
Convert an Existing TCP/IP Port to Equitrac Port

Use the Equitrac Printer Configuration Wizard to convert from a TCP/IP port to Equitrac ports. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports if desired.

To convert from TCP/IP printer ports to Equitrac ports, do the following:

1. Select **Start > All Programs > Xerox Secure Access > Printer Configuration Wizard**.
2. Click **Next** on the Welcome screen to continue with the conversion.
3. Select **Convert printers to use Equitrac Ports**, and click **Next**. Optional – Uncheck **Auto-discover model** if the printers are off-line or have SNMP disabled. If selected, the wizard sends an SNMP request to each device, and then times-out on each failed connection attempt, greatly increasing the time to run the conversion.

4. Select the desired print server(s) from the list, and click **Next**. Optionally, enter the name of other print servers in the Add field, and click the **Add** button to place them in the **PrintServer** list. Print servers can only be added one at a time.

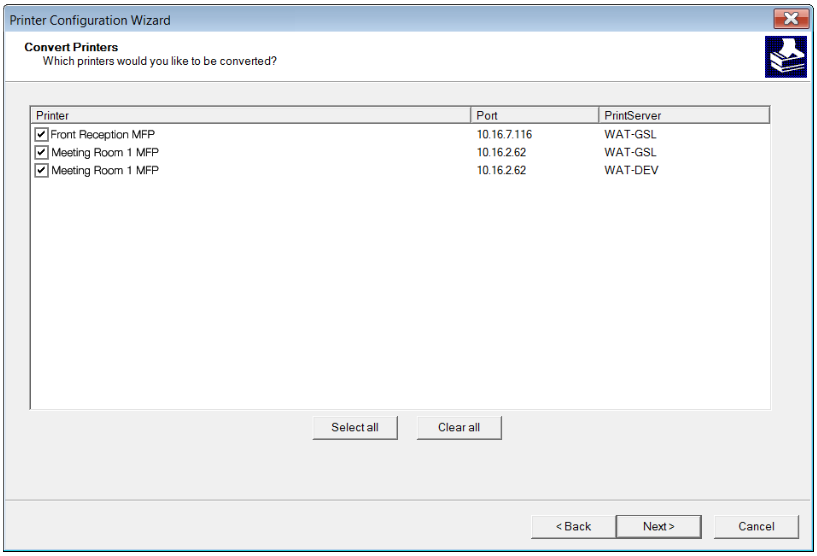


Convert Printers
Select print servers

Print Server
☑ WAT-GSL

WAT-DEV

5. Select the printer(s) to be converted, and click **Next**. If a printer exists on more than one print server, it displays multiple times in the **Printer** list along with the name of its associated server in the **PrintServer** list.

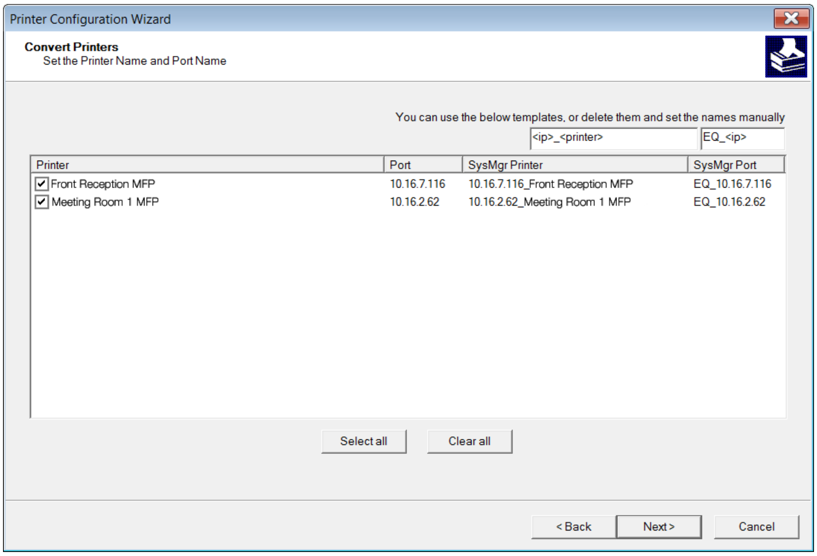


Convert Printers
Which printers would you like to be converted?

Printer	Port	PrintServer
☑ Front Reception MFP	10.16.7.116	WAT-GSL
☑ Meeting Room 1 MFP	10.16.2.62	WAT-GSL
☑ Meeting Room 1 MFP	10.16.2.62	WAT-DEV

6. Set the **Printer Name** and **Port Name** as they will display in the System Manager Devices view. You can use the default naming templates for the printer "**<ip>_<printer>**" and port "**EQ_<ip>**", or change the names as desired.

   For example, you can change the printer default from "**<ip>_<printer>**" to "2nd floor **<printer>**" to associate the selected printer(s) with the 2nd floor in your environment, or remove "**<printer>**" from the name to only display the printer's IP address in System Manager (where <ip> is typed, the printers IP will be automatically replaced; where <printer> is typed, the queue name will be automatically replaced).



Printer Configuration Wizard

Convert Printers

Set the Printer Name and Port Name

You can use the below templates, or delete them and set the names manually

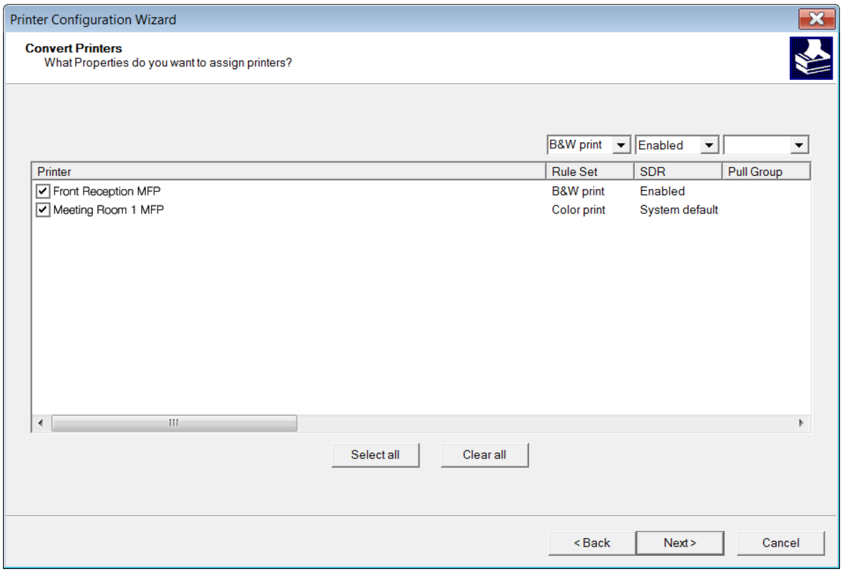
<ip>_<printer> EQ_<ip>

Printer	Port	SysMgr Printer	SysMgr Port
☑ Front Reception MFP	10.16.7.116	10.16.7.116_Front Reception MFP	EQ_10.16.7.116
☑ Meeting Room 1 MFP	10.16.2.62	10.16.2.62_Meeting Room 1 MFP	EQ_10.16.2.62

Note

The printer and port names can be changed individually or as a group. If multiple printers are selected, the naming convention affects the entire selection.

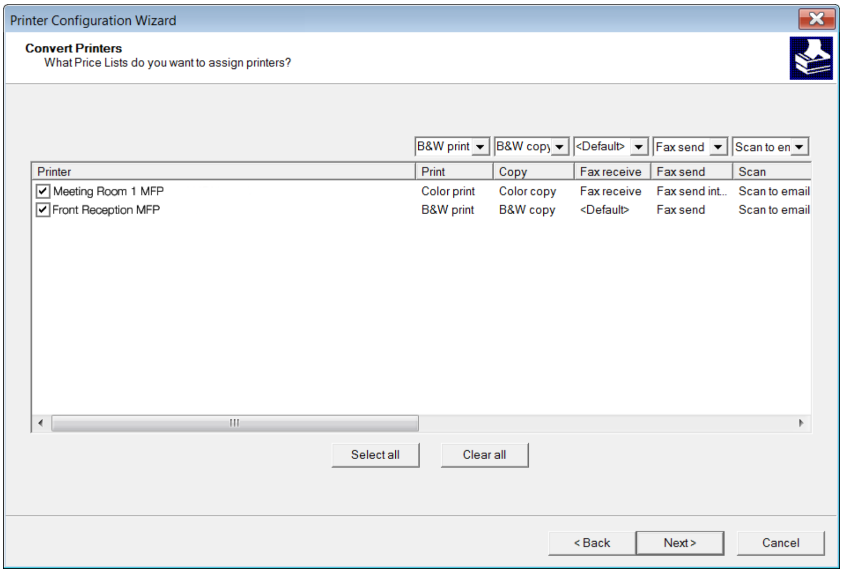
7. On the **Properties** page, select the properties you want to assign to the printers from the Rule Set, SDR and Pull Group drop-down lists. The properties can be applied to single or grouped printers.



Convert Printers
What Properties do you want to assign printers?

Printer	Rule Set	SDR	Pull Group
☑ Front Reception MFP	B&W print	Enabled	
☑ Meeting Room 1 MFP	Color print	System default	

8. On the **Price Lists** page, select the price list. you want to assign from the Print, Copy, Fax receive, and Fax send drop-down lists. The price lists can be applied to single or grouped printers.



Convert Printers
What Price Lists do you want to assign printers?

Printer	Print	Copy	Fax receive	Fax send	Scan
☑ Meeting Room 1 MFP	Color print	Color copy	Fax receive	Fax send int...	Scan to email
☑ Front Reception MFP	B&W print	B&W copy	<Default>	Fax send	Scan to email

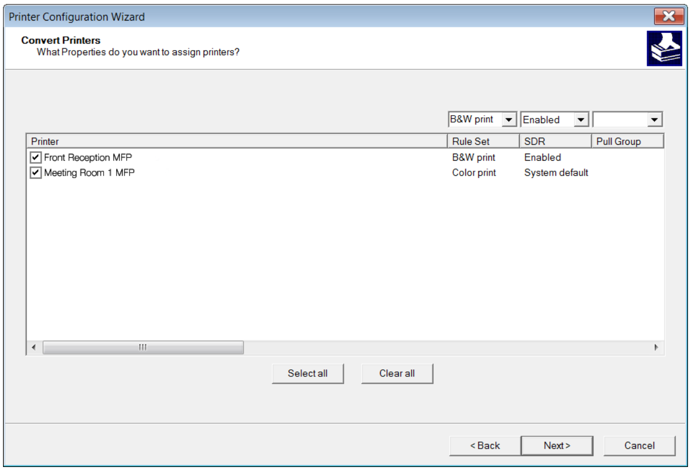
9. Click **Finish** to complete the conversion process. Alternatively, you can select the **Return to Start** checkbox and click **Next** to return to the Wizard's main page without completing the conversion.
10. Open the Printers and Faxes window, and print a test page for EACH converted printer.
11. Confirm that the test page printed successfully.
12. Verify that the physical device and its printer port and print queue display in **System Manager > Devices**.

Configuring Physical Devices with the Configuration Wizard

Use the Printer Configuration Wizard to reconfigure existing printers. The wizard allows for properties such as price lists, rule sets, pull groups and SDR to be set across multiple devices simultaneously.

To configure existing printers, do the following:

1. Select **Start > All Programs > Xerox Secure Access > Printer Configuration Wizard**.
2. Click **Next** on the Welcome screen to continue with the conversion.
3. Select **Configure Equitrac Printers**, and click **Next**. Optional – Uncheck **Auto-discover model** if the printers are off-line or have SNMP disabled. If selected, the wizard sends an SNMP request to each device, and then times-out on each failed connection attempt, greatly increasing the time to run the configuration.
4. On the **Properties** page, select the properties you want to assign to the printers from the Rule Set, SDR and Pull Group drop-down lists. The properties can be applied to single or grouped printers.



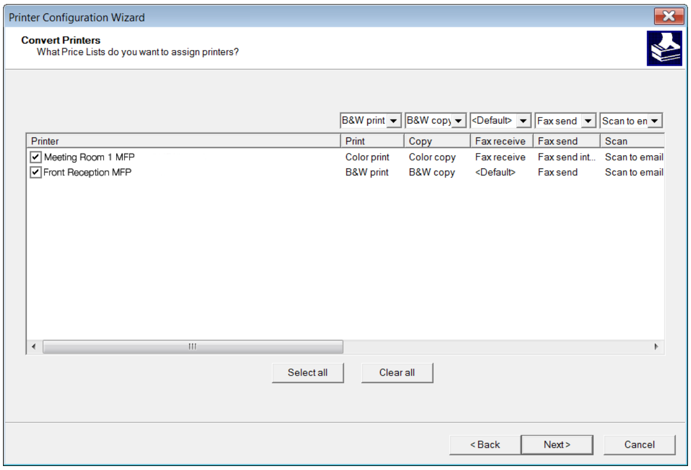
Printer Configuration Wizard

Convert Printers
What Properties do you want to assign printers?

B&W print ▾ | Enabled ▾ | ▾

Printer	Rule Set	SDR	Pull Group
☑ Front Reception MFP	B&W print	Enabled	
☑ Meeting Room 1 MFP	Color print	System default	

5. On the **Price Lists** page, select the price list. you want to assign from the Print, Copy, Fax receive, and Fax send drop-down lists. The price lists can be applied to single or grouped printers.



Printer Configuration Wizard

Convert Printers
What Price Lists do you want to assign printers?

B&W print ▾ | B&W copy ▾ | <Default> ▾ | Fax send ▾ | Scan to en ▾

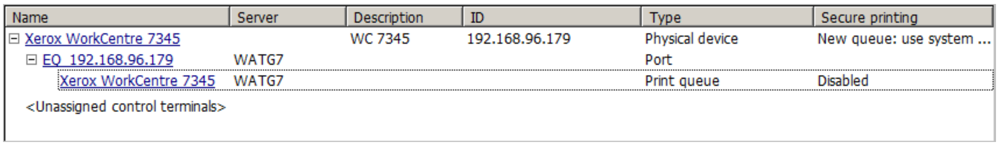
Printer	Print	Copy	Fax receive	Fax send	Scan
☑ Meeting Room 1 MFP	Color print	Color copy	Fax receive	Fax send int...	Scan to email
☑ Front Reception MFP	B&W print	B&W copy	<Default>	Fax send	Scan to email

6. Click Finish to complete the configuration process.

Enabling Secure Printing on the Queue

If you are configuring a secure print environment, the queue must be configured to hold print jobs.

1. In System Manager, navigate to **Configuration** > **Devices.**
2. Click on the Print queue you want to configure. You may need to expand the Physical device to see the print queue.

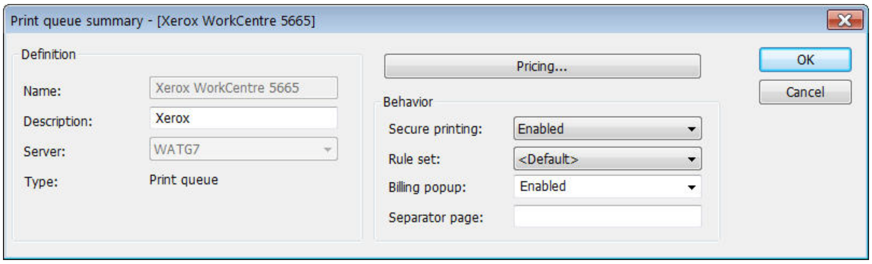


Name	Server	Description	ID	Type	Secure printing
⊟ Xerox WorkCentre 7345		WC 7345	192.168.96.179	Physical device	New queue: use system ...
⊟ EQ_192.168.96.179	WATG7			Port	
Xerox WorkCentre 7345	WATG7			Print queue	Disabled
<Unassigned control terminals>					

Note

The print queue is created automatically the first time a user prints to the controlled device, including when you print a test page upon configuration. If a print queue does not appear beneath the Physical Device, send a print job to the MFP, then wait 30 seconds and refresh System Manager.

3. In the Print queue summary dialog box, set the **Secure printing** option to **Enabled** from the Behavior section, and click **OK**.



Print queue summary - [Xerox WorkCentre 5665]

Definition

Name: Xerox WorkCentre 5665

Description: Xerox

Server: WATG7

Type: Print queue

Behavior

Secure printing: Enabled

Rule set: <Default>

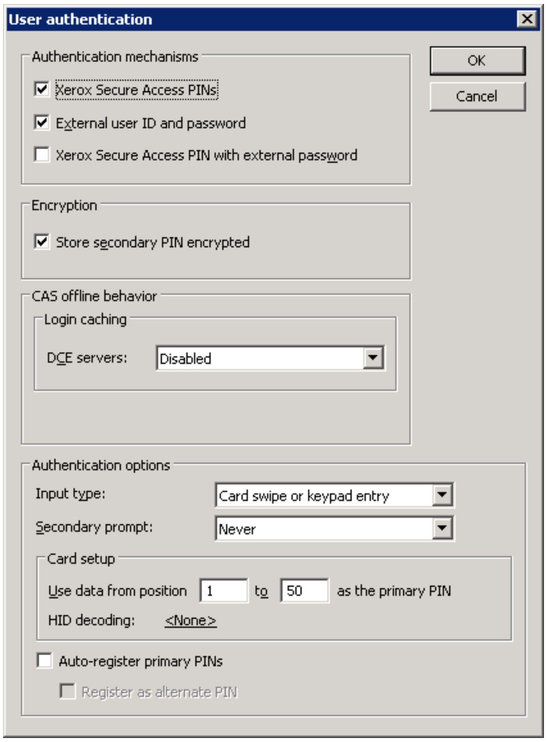
Billing popup: Enabled

Separator page:

Configuring Authentication Prompts

The user authentication prompts on the MFP login screen are determined by your Xerox Secure Access configuration.

1. In System Manager, navigate to **Configuration > User authentication**.



Authentication mechanisms

☑ Xerox Secure Access PINs

☑ External user ID and password

□ Xerox Secure Access PIN with external password

Encryption

☑ Store secondary PIN encrypted

CAS offline behavior

Login caching

DCE servers: Disabled

Authentication options

Input type: Card swipe or keypad entry

Secondary prompt: Never

Card setup

Use data from position 1 to 50 as the primary PIN

HID decoding: <None>

□ Auto-register primary PINs

□ Register as alternate PIN

2. Select one of the following **Authentication options** from the **Input type** drop-down list:
   - **Card swipe only** – Users authenticate with a swipe card.
   - **Card swipe or keypad entry** – Users authenticate with a swipe card or at the MFP front panel.
   - **Keypad only** – Users authenticate at the MFP front panel
3. Select one of the following options from the **Secondary prompt** drop-down list:
   - **Always** – User must enter a secondary PIN via the keyboard after they swipe their card.
   - **If PIN2 available** – User must enter a secondary PIN if they have a PIN 2 value associated with their user account.
   - If PIN2 available or keyboard login – User must enter a secondary PIN if they have a PIN 2 value associated with their user account, or if they entered their primary PIN via the keyboard.
   - **Never** – Secondary PIN is not required.
   - **Only with keyboard login –** User must enter a secondary PIN if they entered their primary PIN via the keyboard (rather than with a swipe card). This option prevents users from typing in someone else's primary PIN while still allowing valid users to login without a card.

Note

If a change is made to the Secondary prompt option, then you must re-initialize the device in order to enable the new selection.

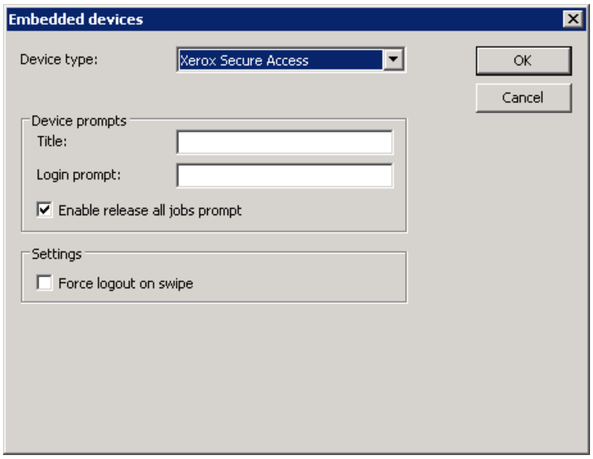
4. In the **Card setup** area, enter the data start and stop positions in the **Use data from position**.
5. Select **Auto-register primary PINs** if you want users to register an unrecognized swipe card for future use. An External authority must be selected to allow card self-registration. See Configuring Card Self-Registration on page 13 for details.
6. Click **OK** to save the change.

For more detailed user authentication options see Accounts System Configuration in the Xerox Secure Access Administration Guide.

Setting Xerox Secure Access Prompts

The following settings must be set before creating Xerox embedded devices.

1. In System Manager, navigate to **Configuration** > **Embedded Devices**.



Embedded devices

Device type: Xerox Secure Access

Device prompts

Title:

Login prompt:

☑ Enable release all jobs prompt

Settings

□ Force logout on swipe

2. Select **Xerox Secure Access** from the **Device type** drop-down list.
3. Enter a **Title** and **Login prompt** to display on the login screen of the embedded device.

Note

If you modify the Title or Login prompt after a device has been initialized by the Xerox Secure Access server, you will have to re-initialize the device again. See Configuring Embedded Devices on page 14 for instructions.

4. Select **Enable release all jobs prompt** if you are not using the Follow-You Printing application and want to prompt for batch release of all jobs.
5. Select **Force logout on swipe** to allow the user to logout by swiping their card a second time.
6. Click **OK** to save the changes.

Configuring Card Self-Registration

f you want users to self-register their swipe cards, you must enable this option in System Manager. When a user swipes an unregistered card, they are required to login to the MFP with valid User ID and Password. The User ID must already exist in CAS, or in the External authority defined to allow self-registration. The Password comes from one of the defined external authorities. The information the user must enter depends upon the authentication options that are set in System Manager. Two-level authentication is required to register new cards, and the user must manually enter both primary and secondary login credentials.

1. Open System Manager and navigate to **Configuration > User authentication**.
2. In the **Authentication options** section, do the following:
   a. Set **Secondary Prompt** to either **If PIN2 available or keyboard login** or **Only on keyboard login** to ensure that the password is prompted during card registration.
   b. Select the **Auto-register primary PINs** checkbox. Optionally, you can select **Register as alternate PIN** to record the PIN as the Alternate PIN instead of the Primary PIN.
3. Select one or more **Authentication mechanisms**:
   - **Xerox Secure Access PINs** – Select to connect an **Xerox Secure Access print** account with login information.
   - **External user ID and password** – Select to verify all user information outside of **Xerox Secure Access.**
   - **Xerox Secure Access PIN with external password** – Select if users swipe their cards for identification, and must also enter their domain user account password. **Xerox** cross-checks the database for the corresponding **Xerox Secure Access** account name, then verifies the credentials against the selected external authority for network logon.
4. Click **OK** to save the changes and close the **User authentication dialog box.**
5. Navigate to **Configuration > External authentication and** select an **External authority** – Windows or LDAP. Refer to External User Authentication in the *Xerox Secure Access Administration Guide* for more details on setting up an external user authentication method.

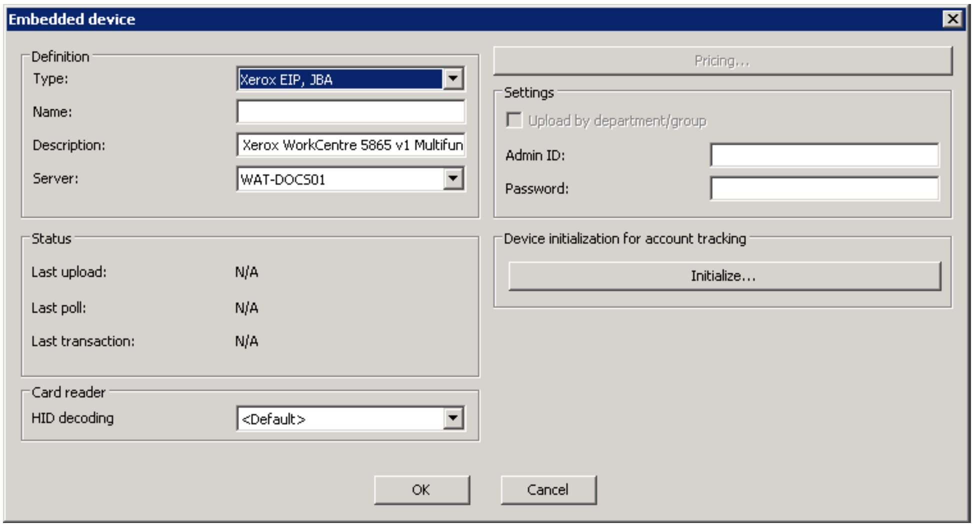
   Once the user registers their card, their account information is automatically associated with that card. The next time the user swipes their card, they can login automatically without manually entering their password. However, if **Secondary prompt** is set to **Always** in System Manager, the user must enter a secondary PIN, or an external authority password after they swipe their card.

Configuring Embedded Devices

Embedded devices are manufacturer-specific software bridges that handle the transfer of user authentication and transaction details between these devices and your accounting server database. Supported devices prompt users for valid user and account ID information for all print release, walk-up copy, and fax jobs.

You must create an embedded interface for each Xerox MFP that will be controlled by Xerox Secure Access. The System Manager component provides the tools to create these interfaces.

1. Open System Manager and select **Devices** in the left pane.
2. Right-click on a Xerox MFP in the right pane, then select **Add embedded device** from the menu.



Embedded device

Definition

Type: Xerox EIP, JBA

Name:

Description: Xerox WorkCentre 5865 v1 Multifun

Server: WAT-DOCS01

Status

Last upload: N/A

Last poll: N/A

Last transaction: N/A

Card reader

HID decoding <Default>

Settings

□ Upload by department/group

Admin ID:

Password:

Device initialization for account tracking

3. Select **Xerox EIP, JBA** from the **Type** drop-down list.
4. Enter a **Name** and **Description** to identify the embedded device.
5. Select the **Server** hosting the DCE associated with the embedded device from the drop-down list.

   Note

   If you change the server associated with an embedded device that has already been initialized by the Xerox Secure Access server, you must re-initialize the device.

6. Select the Card Reader **HID decoding** from the drop-down list.

   For details on HID decoding, see the Xerox Secure Access Administration Guide.

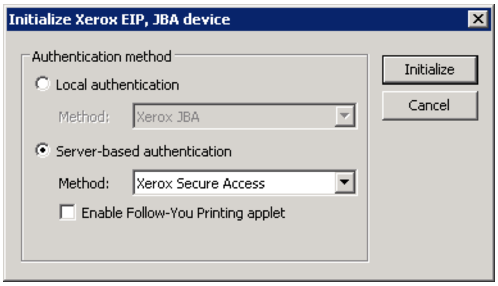
7. Click **Pricing** to configure pricing at the embedded device level.

   For pricing details, see Configuring Price Lists in the *Xerox Secure Access Administration Guide*.

Note

To configure the embedded device to use the price list for that device, select the **default** price list. If you select an alternate price list for the embedded device, the embedded device price list overrides the default price.

8. Enter an **Admin ID** and **Password** to set up secure administrator access to the device. This password and ID must be identical to those used with the eqxeroxeipregistration.exe utility.
9. Click the **Initialize** button to open the Initialize device dialog box.



Initialize Xerox EIP, JBA device

Authentication method

○ Local authentication

Method: Xerox JBA

● Server-based authentication

Method: Xerox Secure Access

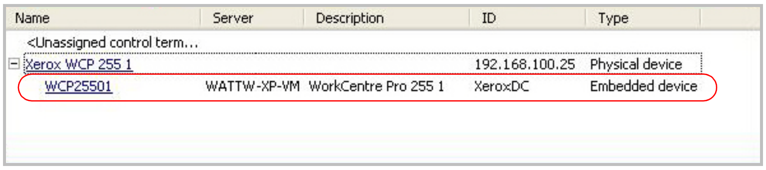
□ Enable Follow-You Printing applet

10. Select the **Server-based authentication** option, and choose a method from the drop-down list.
    - **Xerox Secure Access**– to track printing through Xerox Network Accounting. See Print Tracking Using Xerox Network Accounting on page 26.
    - **Xerox off-box JBA** – to validate prior to processing print activity.
11. Click **Initialize** to configure communication between this device and the Xerox Secure Access server, and return to the Embedded device dialog box.

Caution

Clicking **Initialize** changes the configuration on the device itself and requires some MFPs to reboot. Ensure that the MFP is not in use before you click Initialize. You must manually reboot WorkCentre 52xx, 7232/7242, 73xx, and 74xx models for these settings to take effect. Click the Reboot button on the MFP's web configuration page to accomplish the reboot remotely.

12. Click **OK** to save the embedded device details and close the dialog box. The new embedded device appears in the Devices list beneath the Physical device it is associated with.



Name	Server	Description	ID	Type
<Unassigned control term...				
⊟ Xerox WCP 255 1			192.168.100.25	Physical device
WCP25501	WATTW-XP-VM	WorkCentre Pro 255 1	XeroxDC	Embedded device

13. Repeat these steps to create an embedded device on each supported Xerox MFP in the Devices list.

Note

If initialization fails, and the Xerox device does not appear in System Manager, go back to Configuring Printer Ports on page 4 and confirm that the MFP is properly configured.

After Initialization, log into a Xerox MFP configuration page as the Administrator to verify that the Admin ID and Password entered in System Manager are configured properly. When login is successful, a web page opens displaying the Xerox MFP model name and its settings.

Note

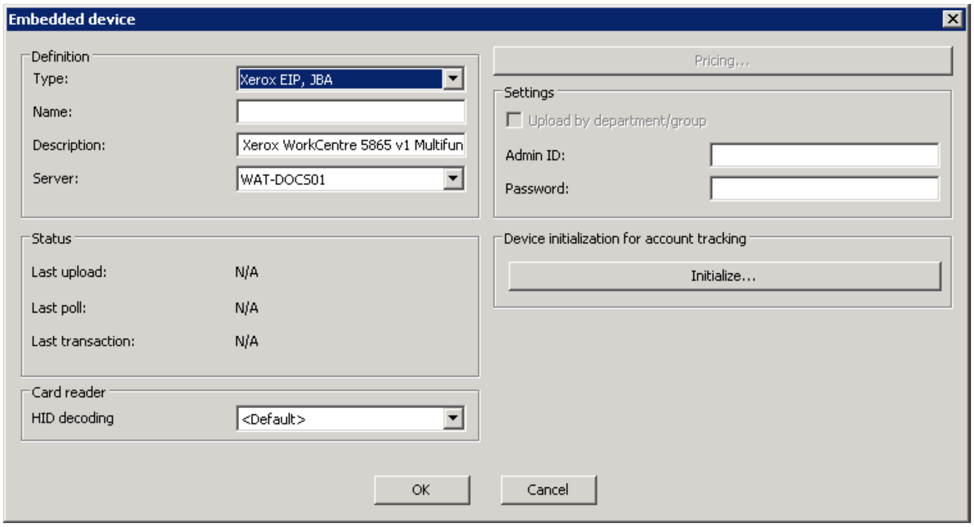
If the MFP is running EIP firmware version 1.5 or 2.0, the **Embedded** Manual Override option must be **Enabled** through the MFP Internet Services Interface in order for the attached card reader to operate normally. See WorkCentre 75xx Series on page 11 for setup details.

Configuring Smart Card Authentication

Embedded devices configured with Smart Card authentication require users to log in using the physical Smart Card and entering a valid userID at the device for all print, copy, and fax jobs.

To configure Smart Card authentication, do the following:

1. Open System Manager and select **Devices** in the left pane.
2. Right-click on a Xerox MFP in the right pane, then select **Add embedded device** from the menu.



Embedded device

Definition
Type: Xerox EIP, JBA
Name:
Description: Xerox WorkCentre 5865 v1 Multifun
Server: WAT-DOCS01

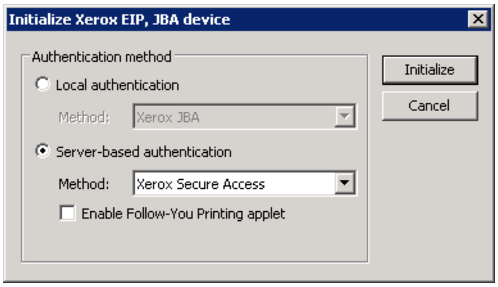
Settings
□ Upload by department/group
Admin ID:
Password:

Status
Last upload: N/A
Last poll: N/A
Last transaction: N/A

Device initialization for account tracking

Card reader
HID decoding <Default>

3. Select **Xerox EIP, JBA** from the **Type** drop-down list.
4. Enter a **Name** and **Description** to identify the embedded device.
5. Select the **Server** hosting the DCE associated with the embedded device from the drop-down list.
6. Select the Card Reader **HID decoding** from the drop-down list. For details on HID decoding, see the Xerox Secure Access Administration Guide.
7. Click **Pricing** to configure pricing at the embedded device level. For pricing details, see *C*onfiguring Price Lists in the *Xerox Secure Access Administration Guide*.
8. Enter an **Admin ID** and **Password** to set up secure administrator access to the device. This password and ID must be identical to those used with the eqxeroxeipregistration.exe utility.
9. Click the **Initialize** button to open the Initialize device dialog box.



Initialize Xerox EIP, JBA device

Authentication method
○ Local authentication
Method: Xerox JBA
● Server-based authentication
Method: Xerox Secure Access
□ Enable Follow-You Printing applet

10. Select the **Local authentication** option, and choose **Xerox Native SmartCard** from the drop-down list.

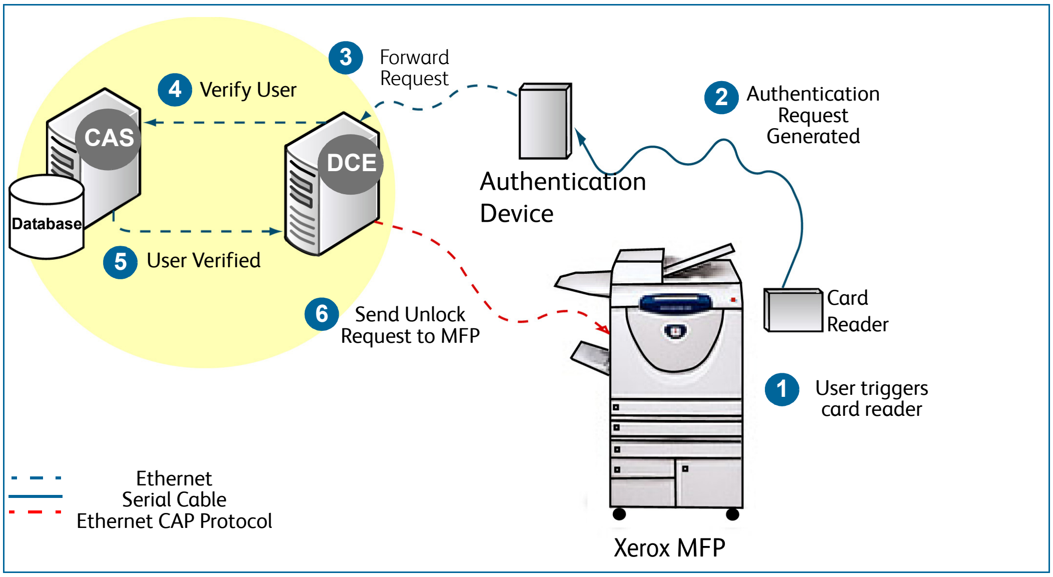
    Caution

    Xerox Print Admin Suite relies upon existing SmartCard functionality to allow authentication for embedded functions. Authentication through SmartCard is dependent upon a pre-existing operational native smart card setup per device. Ensure your setup includes smart card authentication before installing the embedded solution.

11. Select the **Enable Follow-You Printing applet** checkbox to enable Follow-You Printing on the device.
12. Click **Initialize** to configure communication between this device and the Xerox Secure Access server, and return to the Embedded device dialog box.
13. Click **OK** to save the embedded device details and close the dialog box.

Setting Up Authentication Devices

Using a proprietary protocol called Convenience Authentication, the Authentication Device contacts the accounting server via an ethernet network connection to verify the user information gathered from the swipe or proximity card. If the accounting server verifies the user, the MFP device panel unlocks and is ready for use. If the user is not verified, the MFP remains locked and the user cannot perform any tasks at the device. The user can access the Embedded functions only when they are authenticated and the front panel is unlocked.



Setup of each Authentication Device requires a three-step process, outlined below. Before proceeding, ensure that you have all required Authentication Device components. See Authentication Device Component Requirements on page 5.

1. Set the IP Address for each Authentication Device and indicate the DCE IP Address that will communicate with this Authentication Device. Follow Set the Authentication Device IP Address on page 18.
2. Mount the Authentication Device hardware on or near the MFP. Follow Mount the Authentication Device on page 21.
3. Plug in the power, serial, expansion, and card reader connections. Follow Connect the Hardware on page 22.

Set the Authentication Device IP Address

Xerox Authentication Devices are configured for DHCP communication by default. You need to assign an IP Address to each Authentication Device, and set the server IP Address of the DCE component. There are two methods to assign the IP Address:

- Using a DHCP server to assign addresses ensures that the IP Address assignments are handled by the DHCP server when you connect the Authentication Device to the network. However, you need to configure the DHCP server to locate the Authentication Devices. Follow Configure the DHCP Server to Locate the Authentication Devices on page 19.

- If you are not using a DHCP server, or if you prefer not to set option 230 on your DHCP server, you need to use the Authentication Device Web Admin application to set the addresses manually. Follow Manually Assign the IP Address on page 19.

Configure the DHCP Server to Locate the Authentication Devices

1. In Windows Administrative Tools, open the DHCP windows management console.
2. Select the DHCP server root node.
3. From the **Action** menu, select **Set Predefined Options**.
4. From the **Option Class** drop-down list, select **DHCP Standard Options**.
5. In the **Option Name** section, click **Add**.
    a. In the **Name** field, enter **Xerox Secure Access.** This field is used for identification purposes only.
    b. From the **Datatype** drop-down list, select **String.**
    c. In the **Code** field, enter **230.**
    d. In the **Description** field, type: **Secure Access.**
    e. Click **OK**.
6. In the **String Value** section, enter **EQ;A;<DCE Server IP Address>** in the **String** field, where <DCE Server IP Address> is the IP Address of your DCE server. For example:
7. EQ;A; 192.168.100.137
8. Expand the **Scope** node and select **Scope Options**.
9. From the **Action** menu, select **Configure Options**.
10. Select **230**.
11. Click **OK** to save the changes.

Manually Assign the IP Address

❗ Caution

Follow these instructions only if you are not using a DHCP server to set the IP Address of the Authentication Device OR if you are using a DHCP server, but prefer to use static IP Addresses rather than using option 230.

When first powered up, the Authentication Device looks for a DHCP server to secure an IP Address. If no DHCP server is found, the device switches to static communication and defaults to a static IP Address of 192.168.2.1. You can use a standard ethernet cable to connect a system (for example, a laptop) to the Downlink port on each Authentication Device, then use the Web Admin tool to change the IP Address, and enter the DCE Server IP Address.

Print out the Tear sheet found on page 5 before you start. Use this sheet to record the IP Addresses you assign to each Authentication Device.

Configure the Admin Laptop

The system running the Web Admin tool must recognize the static IP Address before you can access the Web Admin tool.

1. On the system (laptop) that will run the Web Admin tool, select **Network Connections > Local Area Connection > Properties**.
2. Double-click **Internet Properties** (TCP/IP), then click **Advanced**.
3. In the IP Addresses section, click **Add**.
4. Enter the following:

   IP Address: 192.168.2.x (where x is an unassigned IP)
   Subnet Mask: 255.255.255.0
5. Click **Add** to save the changes.

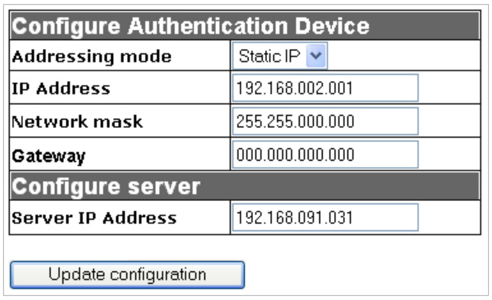
Use the Web Admin Tool to Set IP Addresses:

Perform the following procedure on each Authentication Device.

1. Use a regular Ethernet cable to connect a laptop to the Downlink port on the Authentication Terminal.
2. To power up the Authentication Terminal, attach one end of the AC power cable to the Authentication Terminal, then plug the other end into an available outlet.
3. Open a web browser, and enter **192.168.2.1** in the Address field.

   This is the factory default IP Address assigned to the Authentication Device.
4. Select the **Configure** link at the top of the page.
5. Enter the following to login:

   User name: deviceadmin
   Password: pc_passwd
6. Change the password used to access the Web Admin tool. You can reset the password at any time, but ensure that you change the password from the default setting before the Authentication Device is up and running.
7. In the **Configure Authentication Device** section, choose Static IP from the **Addressing mode** drop-down list.



Configure Authentication Device	
Addressing mode	Static IP
IP Address	192.168.002.001
Network mask	255.255.000.000
Gateway	000.000.000.000
Configure server	
Server IP Address	192.168.091.031

8. Enter a static IP Address in the **IP Address** field to set the address of this Authentication Device.
9. In the **Configure Server** section, enter the DCE Server's IP Address in the Server IP Address field.
10. Click the **Update Configuration** button located below the Configure Server fields.

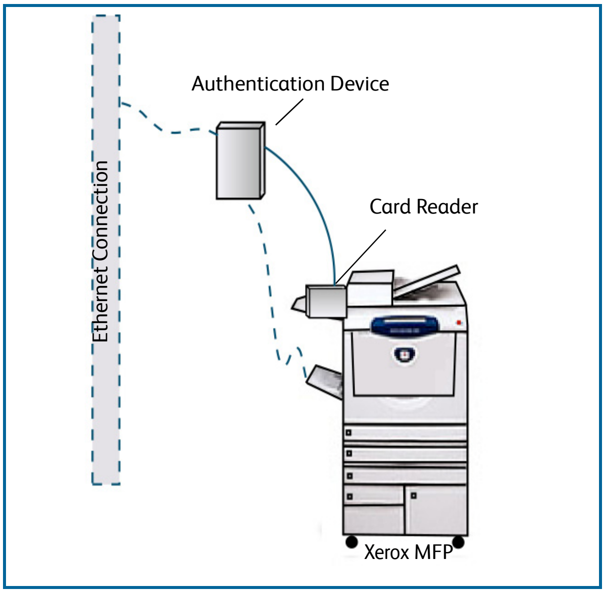
11. Click the **Restart** link at the top of the page, then click “Click here to confirm restart” to restart the terminal.
12. Repeat these instructions for each Authentication Device that you are deploying.

    Note

    Remember to reconfigure the laptop Internet Properties when you are done.

Mount the Authentication Device

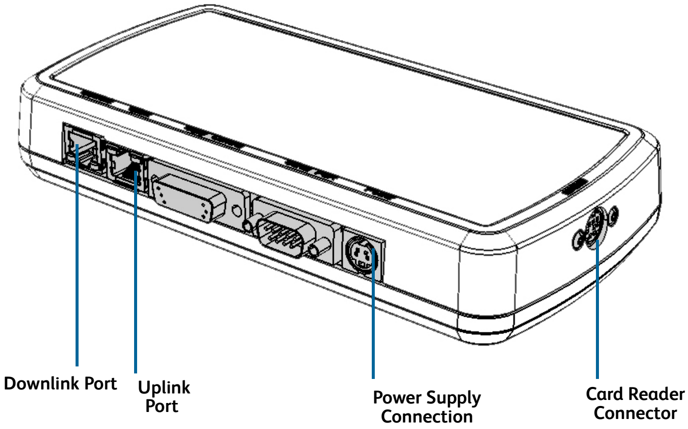
Print out the Configuration Tear Sheet found on page 5. As you work, complete the Authentication Device’s IP Address and MAC Address columns on this sheet. You need this information when you configure communication between devices within System Manager.



1. Lay the Authentication Device on the floor, behind and on the input side of the MFP. The device should be placed in an unobtrusive location, but ensure that the device is placed within 6 feet of the card reader (serial cable length is 6 feet).
2. Mount the Card Reader on the shelf on the left side of the MFP front panel using the supplied Velcro strip. If you have the Convenience Stapler option, place the Card Reader to the right of the stapler so the Card Reader is between the stapler and MFP. Ensure the Document Handler top cover can be opened without being obstructed by the Card Reader before attaching the Velcro strip.
3. Use the Tear Sheet (see page 5) to record the IP and MAC Address of the MFP that this Authentication Device will control.

Connect the Hardware

Using the labeled graphic below for reference, connect the components. Note that the Authentication Device provides a serial port and a copy control port that is not used in this configuration.



1. Use the Tear sheet to record the MAC address of the Authentication Device. Enter this address in the same row as the MFP it will control.
2. Plug the Card Reader serial cable into the Card Reader connector on the Authentication Device.
3. Connect one end of the Ethernet cable into the network drop and the other end into the Uplink port on the Authentication Device.
4. Connect the MFPs ethernet cable to the Downlink port on the Authentication Device.

   Note

   When the Authentication Device is powered off, there is no Ethernet connectivity available from the Downlink port. Alternatively, you can plug the MFP Ethernet cable directly into another Ethernet port. The Downlink port is provided on the Authentication Device for situations when another Ethernet port is not available.

5. Connect the power supply to the Authentication Device, then plug the other end into the nearby receptacle.

The physical hardware setup of the Authentication Device is now complete. Repeat these instructions for each Authentication Device.

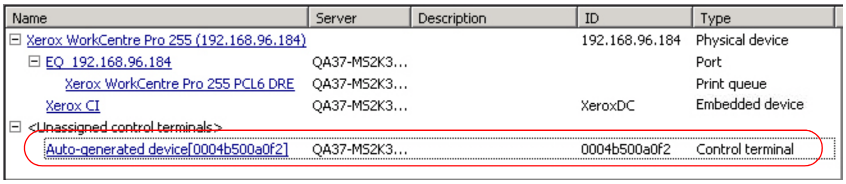
Note

The Authentication Device does not control access to an MFP until you perform an association in System Manager, described below.

Associating Authentication Devices with MFPs

When you initially power on an Authentication Device connected to the network, the DCE registers the device. The DCE then forwards the configuration details to the accounting server, and the Devices list in System Manager updates accordingly.

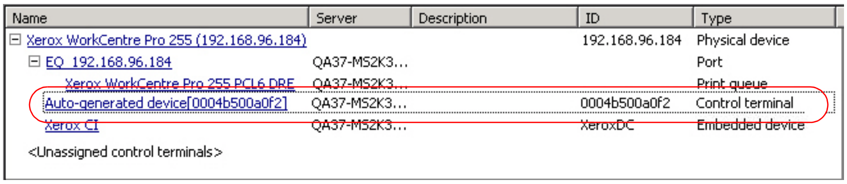
Unassigned Authentication Devices appear in the Devices list under the <Unassigned control terminals> section (using the Standard view in the Devices window).



Name	Server	Description	ID	Type
Xerox WorkCentre Pro 255 (192.168.96.184)			192.168.96.184	Physical device
EQ_192.168.96.184	QA37-MS2K3...			Port
Xerox WorkCentre Pro 255 PCL6 DRE	QA37-MS2K3...			Print queue
Xerox CI	QA37-MS2K3...		XeroxDC	Embedded device
<Unassigned control terminals>				
Auto-generated device[0004b500a0f2]	QA37-MS2K3...		0004b500a0f2	Control terminal

Each Authentication Device is labelled as “Auto-generated device”, but can be differentiated by MAC Address. Use your Tear sheet to determine which Authentication Device MAC Address maps to the corresponding MFP IP Address.

1. Open System Manager and select **Devices** in the left pane.
2. To associate an Authentication Device with a Physical Device (MFP), simply drag and drop the terminal to the Physical Device. The Authentication Device will then appear below the Physical device.



Name	Server	Description	ID	Type
Xerox WorkCentre Pro 255 (192.168.96.184)			192.168.96.184	Physical device
EQ_192.168.96.184	QA37-MS2K3...			Port
Xerox WorkCentre Pro 255 PCL6 DRE	QA37-MS2K3...			Print queue
Auto-generated device[0004b500a0f2]	QA37-MS2K3...		0004b500a0f2	Control terminal
Xerox CI	QA37-MS2K3...		XeroxDC	Embedded device
<Unassigned control terminals>				

Users must now authenticate to use the MFP. See User Workflow on page 1 for instructions that you can provide to end-users.

Configuring Print Tracking

There are two methods to track printing—through Equitrac ports or through the Xerox client driver popup (also called Xerox JBA or Job-based Accounting). Read the descriptions below to determine the appropriate print tracking setup for your environment.

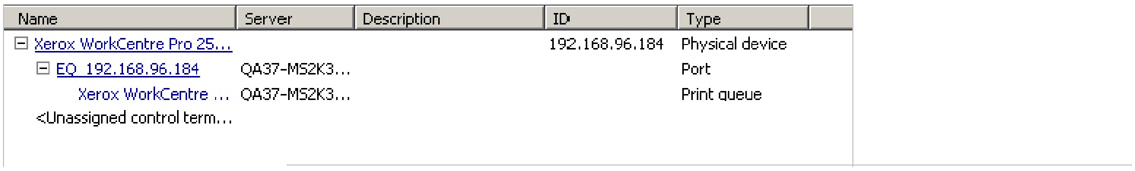
Print Tracking Through Equitrac Ports

When DRE is set to track printing, it gathers details when the user submits a print job. When a job is released, DRE forwards these details to CAS based on the job characteristics determined by the Equitrac Port monitor.

The job details are gathered by the Port Monitor when the user releases the print job at a device. If the user decides to cancel the print job mid-way through printing, or if the user originally selected color printing but the final output device cannot print in color, the precise page details are not captured at the time of output and therefore tracking may not be fully accurate.

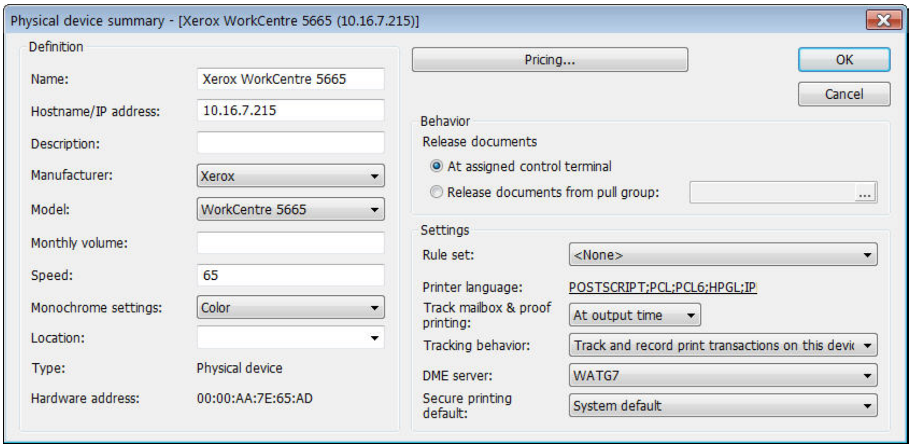
Enable tracking from the physical device

1. Open System Manager and select **Devices** in the left pane.
2. Select the physical device to open the Physical device summary dialog box.



Name	Server	Description	ID	Type
⊟ Xerox WorkCentre Pro 25...			192.168.96.184	Physical device
⊟ EQ_192.168.96.184	QA37-MS2K3...			Port
Xerox WorkCentre ...	QA37-MS2K3...			Print queue
<Unassigned control term...				

3. In the **Settings** area, ensure **Track and record print transactions on this device is selected from the Tracking Behavior** drop-down list. This is the default setting.



Physical device summary - [Xerox WorkCentre 5665 (10.16.7.215)]

Definition

Name: Xerox WorkCentre 5665

Hostname/IP address: 10.16.7.215

Description:

Manufacturer: Xerox

Model: WorkCentre 5665

Monthly volume:

Speed: 65

Monochrome settings: Color

Location:

Type: Physical device

Hardware address: 00:00:AA:7E:65:AD

Pricing...

Behavior

Release documents

● At assigned control terminal

○ Release documents from pull group: ...

Settings

Rule set: <None>

Printer language: POSTSCRIPT;PCL;PCL6;HPGL;IP

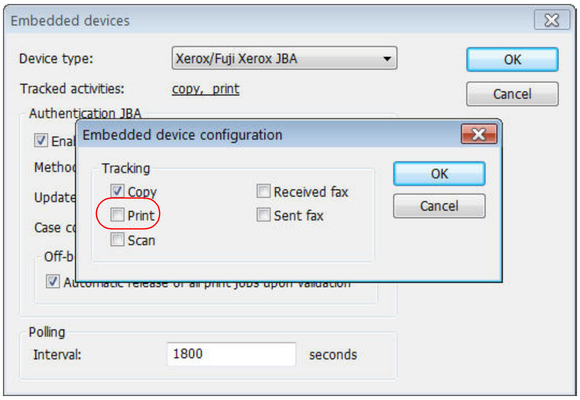
Track mailbox & proof printing: At output time

Tracking behavior: Track and record print transactions on this devic

DME server: WATG7

Secure printing default: System default

4. Click OK to save the changes.
5. Navigate to **Configuration > Devices > Embedded devices**.
6. Select **Xerox/Fuji Xerox JBA** from the Device Type drop-down list.
7. Click on the link beside **Tracked activities** to open the Embedded device configuration dialog box.
8. Ensure that **Print** is **NOT** selected, then click **OK**.



Embedded devices

Device type: Xerox/Fuji Xerox JBA

Tracked activities: copy, print

Authentication JBA

☑ Enal

Methoc

Update

Case c

Off-b

☑ Automatic release of all print jobs upon validation

Polling

Interval: 1800 seconds

Embedded device configuration

Tracking

☑ Copy

□ Print

□ Scan

□ Received fax

□ Sent fax

Print Tracking Using Xerox Network Accounting

When tracking print jobs through a Xerox embedded device, configure the device and its print drivers to accept only authenticated print jobs. Users are prompted to enter user and account credentials prior to printing. The user authentication data is checked by the Xerox device when it receives the print job. The embedded device tracks printing and captures appropriate accounting information.

Use this method when you require precise job accounting. When the user releases a print job, the precise output details are gathered and held at the device after the job is completed. If the user cancels mid-way through a job, or if the device is not capable of producing output as the user intended (i.e. duplex was selected, but the device is not capable of duplexing and produces single-sided output only), the device calculates the precise output details only after the job is fully processed.

The DCE obtains the transaction details from the output device and forwards them to the CAS at a later interval.

This method requires additional configuration steps and your Xerox devices must meet the following prerequisites:

- JBA-supported Xerox device with the Network Accounting module installed and enabled and Authentication (Network Accounting option) enabled.
- TCP/IP enabled and configured on the devices.
- A static IP Address or reserved DHCP IP Address (recommended).
- TCP/IP port 443 communication enabled on the network between the Xerox Secure Access server and the devices.
- Depending on the Xerox device and server operating system, you may require Xerox Advanced Services Management before you can enable the Accounting option on the printer driver. See the Xerox device documentation for details.
- Off-printer (also called off-box) validation must be configured on the Xerox Secure Access server. This option forces the device to send a request to Xerox to validate the data input by the user.
- For Xerox devices to accept authenticated print jobs and the embedded device to track print jobs correctly, the Xerox device and Xerox print drivers must be configured as described in the following table.

Device and Print Driver Configuration	Notes
The **Network Accounting** module must be installed and enabled on each Xerox device.	Xerox Secure Access does not support the Internal Auditron authentication method. When you set the authentication mode on the device, ensure you select the **Network Accounting** option.
The **Network Accounting Configuration > Authentication** option must be enabled.	Depending on the Xerox device Authentication configuration, job information can be accurately tracked by the Xerox device regardless of whether or not the user and account information exists on that device. See the Xerox device documentation for details on configuring options for the physical device.

Device and Print Driver Configuration	Notes
Installed Xerox print drivers must have the **Accounting** option enabled for each printer to prompt users for user and account ID prior to printing.	The location of the Accounting option in the Xerox print driver dialogs may not be the same for all printer connections you create. The option may be located on the **Properties > Document Details** or the **Printer Preferences** dialogs. You may find that the location of the **Accounting** option varies by Windows platform, driver language type (Postscript or PCL), driver version, or device model. The Xerox device deletes print jobs to prevent anonymous (un-billable) printing when any of the following situations apply: • The Xerox print driver does not have authentication features. • The **Accounting** option for the print driver is disabled.
The device must use an Equitrac Port if configuring secure document release.	Secure Document Release is enabled through Equitrac Ports only. Regardless of the print tracking method you choose, you must establish an Equitrac Port on the device if you plan to hold documents for secure release.

Once the prerequisites and configuration steps are complete, you must disable tracking on the physical device.

4

User Workflow

Topics

This section provides end-user instructions for authenticating and using the Embedded functions at the Xerox MFP.

Authenticating at a Card Reader

When Xerox Secure Access controls an MFP, users must authenticate with a magnetic stripe card, proximity card, or smart card before they are able to use the device functions.

Authenticating with a Magnetic Stripe Card

1. Insert the card into the guide track with the magnetic stripe facing the indicated direction. Ensure the card is pressed firmly against the guide.
2. Pull the card down through the guide track and remove the card.

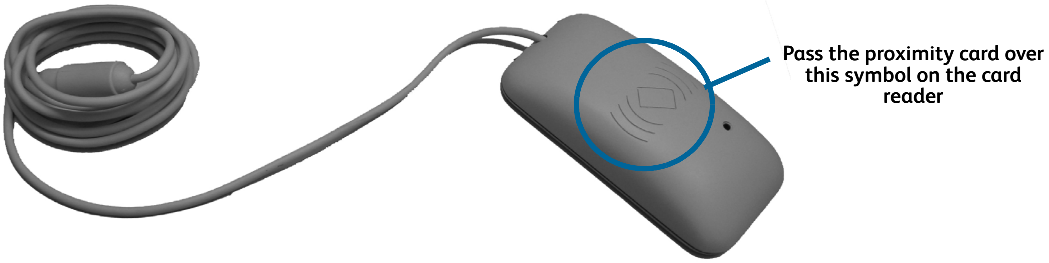
   Note

   Do not run the card through at an angle or the terminal will not accept the data.

3. If the terminal cannot read the entry, the LED flashes red. Reinsert the card into the guide track and run the card through the reader again.
4. If **Secondary prompt** is enabled in System Manager, and a secondary PIN has been assigned in the database, the user **must** enter their ‘password’ on the MFP front panel when prompted. If the user has not been assigned a secondary PIN in the database, they can leave the field blank to proceed.

Authenticating with a Proximity or Smart Card

To enter data using a proximity card or smart card, pass the card within 1 inch or 2.5 cm of the proximity symbol located on the top of the card reader device. To locate the proximity card reader on the data reader module, look for this symbol:

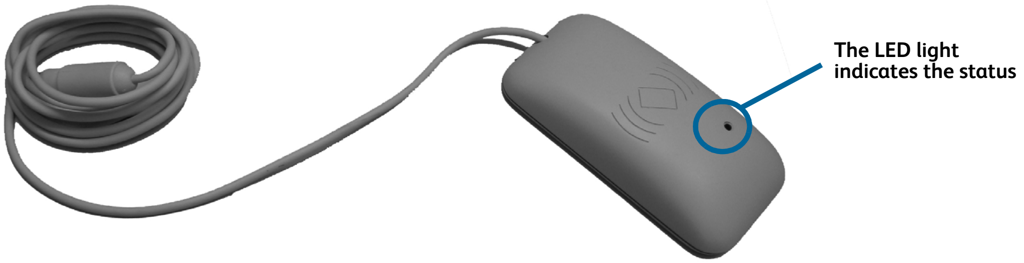


If the swipe is invalid, the LED flashes red.

If secondary PINs are enabled, the user must enter their ‘password’ on the MFP front panel when prompted. If secondary PINs are enabled, but the user has not been assigned a secondary PIN, the user can leave the field blank to proceed.

Card Reader Status Messages

Xerox Secure Access displays its authentication messages through an LED light on the card reader module.



The following signals may be displayed on the card reader:

LED Behavior	Meaning
Solid red	MFP is in Idle mode; it is ready but there is no active session.
Solid green	MFP is in Ready mode and a session is active.
Slow flashing green	Data received from card reader, awaiting authentication for active session. The light continues to flash green until the user enters their secondary PIN at the front panel. If the time-out expires and the user does not enter their PIN, the LED changes back to solid red and the device remains locked.
Slow flashing red	No communication between card reader and MFP.

The MFP has two functional modes, Idle mode or Ready mode.

Idle Mode

An MFP that is ready for use is in Idle mode. When a user passes a key fob or swipes a magstripe card, the device changes to Ready mode.

The MFP returns to Idle mode when:

- A user completes a transaction
- After a specified period of inactivity in Ready mode (Sleep Mode Timer, as configured on the device)
- The user logs out

When the device is in Idle mode, the LED light on the card reader is solid red.

Ready Mode

When the device is in Ready mode, the LED light on the card reader is solid green and the user can begin using the controlled device to perform a transaction.

Logging In to a User Session

A user session begins when the user logs in with valid credentials through the MFP device interface. Once their login credentials have been authenticated, the user can manage and release documents via Follow-You Printing®, or they can access any of the other device features, such as copying, scanning and faxing.

There are two authentication methods available to validate users at a Xerox MFP:

- **Local authentication** - users are authenticated at the Xerox device. For example, the Xerox Smart Card solution uses local authentication. See Configuring Smart Card Authentication on page 16.
- **Server-based authentication** - users are authenticated by CAS. See Configuring Embedded Devices on page 14 for details.

Smart Card Authentication

To authenticate through Xerox Smart Card, do the following:

1. The user inserts their Smart Card into the Xerox supported card reader to open the MFP Login screen.
2. On the Login screen, the user enters their user PIN.
3. On the All Services screen, the user can access any of the native device features (e.g. copy or fax), of they can touch **Custom Services** to access Follow-You Printing. See Using Follow-You Printing® on page 5.

Server Authentication

To authenticate through Xerox Secure Access, do the following:

1. On the Login screen, the user enters their User ID or swipes their card. If System Manager is configured to prompt for Secondary PIN, the user may also need to enter a password.

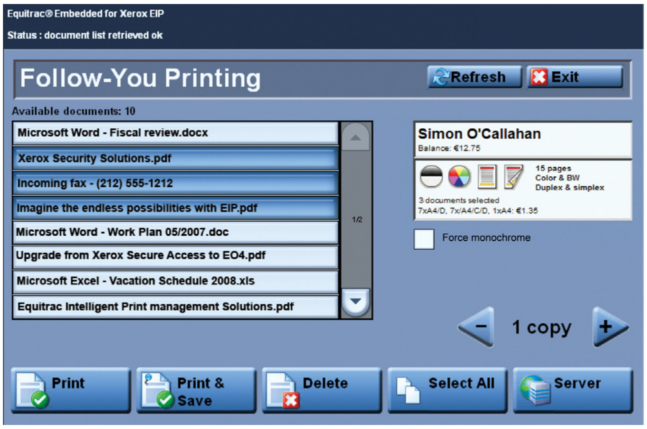
   Depending on how System Manager is configured, one of the following occurs after user authentication:

   - The MFP All Services screen opens, and the user can proceed to the Follow-You Printing application to release their documents.
2. On the All Services screen, the user can access any of the native device features (e.g. copy or fax), of they can touch **Custom Services** to access Follow-You Printing. See Using Follow-You Printing® on page 5.

Using Follow-You Printing®

Users can use Follow-You Printing to release documents held in the print queue associated with the user's account from any device within a predefined pull group, which is connected to the particular print server. Multi-Server Follow-You Printing allows users to select any remote print server accessible to the device within a predefined pull group, and pull documents for printing

1. On the MFP Login screen, the user enters their user credentials or swipes their card. See Smart Card Authentication on page 4 or Server Authentication on page 4 for login options.
2. On the All Services screen, the user touches **Custom Services**.
3. On the Custom Services screen, the user touches **Follow-You Printing** (or **Release Documents** on some devices). The Follow-You Printing screen opens.



Equitrac® Embedded for Xerox EIP

Status : document list retrieved ok

Follow-You Printing

Available documents: 10

- Microsoft Word - Fiscal review.docx
- Xerox Security Solutions.pdf
- Incoming fax - (212) 555-1212
- Imagine the endless possibilities with EIP.pdf
- Microsoft Word - Work Plan 05/2007.doc
- Upgrade from Xerox Secure Access to EO4.pdf
- Microsoft Excel - Vacation Schedule 2008.xls
- Equitrac Intelligent Print management Solutions.pdf

Simon O'Callahan
Balance: €12.75

15 pages
Color & BW
Duplex & simplex

3 documents selected
7xA4/D, 7x/A4/C/D, 1xA4: €1.35

□ Force monochrome

1 copy

4. On the Follow-You Printing screen, the user can perform the following functions at the device:

Function	Description
Print	Touch one or more documents in the list, then touch **Print** to print the documents and delete the jobs from the list.
Print & Save	Touch one or more documents in the list, then touch **Print & Save** to print the documents but keep the jobs in the list.
Delete	Touch one or more documents in the list, then touch **Delete** to remove the jobs from the queue without printing them.
Select All	Selects all jobs in the list, after which you can touch **Print**, **Print & Save**, or **Delete**.
Server	If multiserver Follow-You Printing is enabled on the Xerox Secure Access server, touch **Server** to display a list of authorized network print servers. If you select another server from the list, the Follow-You Printing screen refreshes to show any print jobs waiting on the other server. If multiserver Follow-You is not enabled, you will only see the local server listed. For multiserver Follow-You Printing configuration information, see the “Advanced Printing Configuration” chapter in the Xerox Secure Access Administration Guide.
Refresh	Contacts the DCE server to determine if any new pending jobs are available for the current user. If any print jobs are found, they are added to the bottom of the document list.
Exit	Returns to the MFP Service screen.
Force Monochrome	Allows a user to force a color job to print in black & white.
Number of Copies	Touch the Plus (+) and Minus (-) buttons to change the number of copies for the selected print job(s). If the number of copies is changed at the MFP, a confirmation page appears verifying the number of copies to print. Touch **OK** to continue, or **Cancel** to leave the number of copies at 1. **Note:** By default, the number of copies is reset to 1 after the selected job prints. If more than 1 copy is desired for additional print jobs, the number of copies must be set again before the next job is released.

5. The user touches **Exit** to end the user session and return to the Custom Services screen.

Logging Out of a User Session

While in the Follow-You Printing screen, the user must first touch **Exit** to return to the Custom Services screen, then touches **Close** to return to the main screen on the MFP.

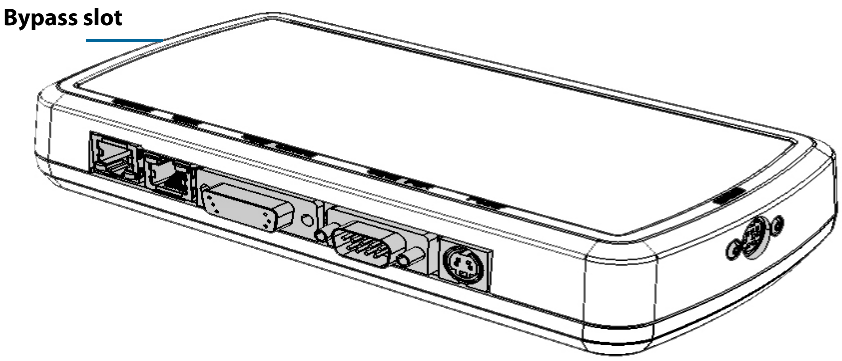
To fully log out of an active session, the user touches the **Clear All** button beside the panel keyboard, then chooses **Log out** in the confirmation dialog box.

If using the Smart Card solution, the user can simply remove their Smart Card to end the user session and completely log out of the device.

Resetting an Authentication Device

Use the metal bypass key to reset the Authentication Device to the default settings. This key was provided with the device and should be stored in a safe place.

1. Ensure the Authentication Device is powered on.
2. Insert the bypass key into the key slot.



3. Holding the device as shown above, turn the key a quarter turn TOWARD you.
4. After 5 seconds, turn the key back to the original position.
5. Ensure the key is fully back in its original position, then remove the key.

   Note

   The device will beep every 10 seconds if the key is not turned back to its original position before you remove the key.

5 Troubleshooting

Before contacting Technical Support for assistance, refer to the following table for symptoms that match the problem you are experiencing. Instructions for possible solutions are also provided.

Symptoms and Solutions

If you experience a problem with your Xerox Secure Access application at a device, refer to the table below for symptoms and solutions that match your problem before contacting Technical Support for help.

Symptom	Possible Resolution
The indicator light on the card reader is off	When the light is not lit, this indicates a loss of power to the reader. Check the cable connection to the Authentication Device and ensure that it is firmly seated. If the light remains unlit, check the power to the Authentication Device. If the Authentication Device does not have power, neither does the card reader.
The Authentication device does not have power	To determine if the unit has power, check the back (connector side) of the unit. A yellow indicator light next to the jack marked “Ethernet” should be lit. If this light is not lit, ensure that the power supply cable is firmly seated in the Authentication Device, and that the power cord is plugged into the power supply brick and into the A/C wall jack. If the light is still not lit, verify that the wall jack has power.
The card reader indicator light is flashing red slowly	The Card Reader is working correctly; however, the Authentication device has failed to connect to the Xerox Secure Access server. Ensure that the Ethernet cable is connected to both the Ethernet port on the Authentication Device and to the wall Ethernet jack. If the Ethernet link light on the Authentication Device flashes green when you first swipe your card, the Ethernet is active, and the problem is likely server-side. Ensure that the Authentication Device has been assigned to the correct MFP. See Associating Authentication Devices with MFPs on page 23 for instructions.

Symptom	Possible Resolution
The card reader indicator light rapidly flashes red upon swipe	The swipe was invalid at the card reader. The Xerox Secure Access server has determined that the card ID does not correspond to a valid user on the network. Test the reader with another card for a user whose card is known to work at other readers. If the cards are not being read correctly at any reader, server configuration may be the cause. Read Configuring Authentication Prompts on page 11 to ensure the card data positions are set correctly.
The card reader indicator light stays red upon swipe	If the indicator light does not change color when you swipe, the reader has not detected the card. Verify that the swipe was performed correctly. A magnetic card may have been encoded with a different standard or swiped upside down or facing the wrong direction; a proximity card or contactless smart card may not have been placed close enough to the reader, or may not be a supported card type. If the same card works at other readers at the same site, the reader module may be at fault. If the card does not work at other readers, verify the card technology with the card vendor and reference Supported Card Readers on page 6.
The Ethernet link light on the Authentication Device is off	There is no Ethernet connection. Verify the Ethernet patch cable and verify that the Ethernet wall jack is active.
The Ethernet link light on the Authentication Device is solid green (as opposed to flashing)	There is Ethernet connectivity, but no activity. Ensure that the Ethernet wall jack is connected to the correct hub or switch.
The Authentication Device is not listed in **System Manager > Devices**	Authentication Devices appear in the Devices list by MAC Address. Check the list of <Unassigned control terminals> to check for the IP Address of the Authentication Device in question. If you cannot locate the correct MAC Address, the DCE Server has not located the device on the Ethernet. If you manually configured the Authentication Device (without DHCP) ensure that you entered the correct DCE IP Address in the Web Admin utility. If you allowed DHCP to assign an IP Address, ensure the Authentication Device is connected to the Ethernet and powered on. You may need to wait approximately 60 seconds for the DCE to contact the device and communicate with the Core Accounting Server before it can populate the Devices list. Also check to ensure that the DHCP server sets value 230 to the DCE Server's IP Address. Ensure the Authentication Device is powered on.
Cannot connect to the Authentication Device's web page	If you set the IP Address manually, check the Tear sheet to ensure you are entering the correct IP Address. If the address looks correct, either the device is not connected correctly, it cannot communicate, or the IP Address was recorded incorrectly. To check the device connection, use an Ethernet cable to connect the Downlink Port on the Authentication Device directly to a PC. If the connection is established, verify the network settings and IP Addresses set for both the Authentication Device itself and the DCE Server. If you cannot connect to the device using an Ethernet cable, reset the Authentication device. See Resetting an Authentication Device on page 7 for instructions. Perform the Authentication Device setup and configuration again. If the web page is still unreachable, the Authentication terminal may be defective.
The Authentication Device beeps at a frequent interval	The bypass key was not returned to its correct position before the key was removed. See Resetting an Authentication Device on page 7 for instructions on correctly resetting the device.

Symptom	Possible Resolution
After the user authenticates at the MFP, an error message appears stating “access to copy job denied”.	A copy rule has been applied to the user and device. The user is not authorized to use the copy function on this device. The user can touch Yes or Exit to logout. For more information on copy rules, refer to the Routing Rules chapter in the *Xerox Secure Access Administration Guide.*
Device initialization failed	A common cause of device initialization failure is due to incorrect DNS configurations. To determine where the error has occurred, run the **EQXeroXEIPRegistration.exe** file located in the Xerox Secure Access Tools folder. This program will produce a verbose error description that will help you diagnose the problem. If DNS configuration is the problem, this file allows you to change DNS addresses into IP Address registrations. Run the executable from a command prompt, followed by /h to view a list of options.
What trace logging settings are required by Support?	In case of failure to initialize Xerox devices, failure to initialize Xerox Secure Access Authentication devices, undesirable authentication behavior, or undesirable network accounting behavior, enable all XeroxDC items within the CAS and DCE logs.

Configuration Tear Sheet

Tear this sheet out and use it when performing the physical setup of the Authentication Devices. You must keep careful track of the IP and MAC Address of each Authentication Device and the corresponding MFP that it will control. The MAC Address of the Authentication Device is printed on the serial number label.

	Authentication Device		Multifunction Device	
	MAC Address	IP Address	IP Address	Hostname
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				